АНАЛИТИЧЕСКАЯ ЗАПИСКА

КОМАНДА «ЭКОНОМИЧЕСКИЙ АЛЬЯНС»

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ

КЕЙС «Искусственный интеллект, большие данные

и безопасность расчетов и платежей (регулятор)»

Авторы:

Кузнецов Александр Алексеевич, СФУ

twinky0405@gmail.com

Немцев Максим Игоревич, СФУ

ifelser.ma@gmail.com

Смолик Михаил Александрович, СФУ

mixail_smolik_sma@mail.ru

Тоденберг Андрей Дмитриевич, СФУ

peugeot30811@gmail.com

Преподаватель-тренер:

Маслова Наталья Валерьевна, преподаватель Кафедры экономической теории ИЭГУиФ СФУ

natmaslova@mail.ru

Красноярск 2022

Введение

Развитие банковской сферы идёт в ногу с развитием современных технологий. Результатом совместного развития становятся системы обслуживания и консультирования граждан, наделённые алгоритмами искусственного интеллекта. Подобные системы были представлены ведущими игроками рынка, такими как «Сбер» и «Тинькофф».

По данным ЦБ был зарегистрирован резкий рост количества фишинговых атак, с 273 в 2020 году, до 1995 – в 2021. В 3 квартале 2021 года было зарегистрировано 256 тысяч операций без согласия потребителя, которые нанесли ущерб на сумму в более чем 3,2 миллиарда рублей, из которых вернуть удалось только 7,7% [33]

Увеличение уровня активности мошенников побуждает банки финансировать новые способы защиты средств граждан, в том числе включающих в себя антифрод-системы, основанные на алгоритмах машинного обучения. Особую актуальность данной теме придаёт повсеместное внедрение подобных систем крупными игроками финансового сектора.

В кейсе «Искусственный интеллект, большие данные и безопасность расчетов и платежей» представлена проблема неэффективности ИИ в области консультации и обслуживания граждан, защиты банковских счетов от мошеннических операций, а также несовершенства законодательной базы в области регулирования деятельности ИИ.

Целью нашей работы является полноценный анализ предложенного кейса, создание решений поставленных задач и предложение мер для улучшения качества работы ИИ и контроля за его деятельностью.

Для достижения поставленной цели были определены следующие задачи:

1. Подробно изучить внутренний и зарубежный опыт применения ИИ в сфере противодействия актам мошенничества.
2. Провести детальный разбор политики Центробанка в отношении развития систем искусственного интеллекта в банковской сфере.
3. Проанализировать имеющуюся нормативную базу, напрямую оказывающую влияние на применение ИИ для противодействия мошенникам.
4. Предложить меры, направленные на поддержание и развитие искусственного интеллекта.

Информационной базой для анализа кейса послужили законодательные и нормативные акты Российской Федерации, судебная практика, общедоступные публикации в сети Интернет, а также статьи периодических изданий и статистические материалы.

Детальный анализ кейса

Основной проблемой, рассматриваемой в кейсе, является несовершенство искусственного интеллекта в сфере антифрода, которые привели к ошибочному срабатыванию механизмов защиты банковского счёта. Показательной ошибкой стала пропущенная транзакция на 399 долларов в Нью-Йорке, которая ярко свидетельствует о **несовершенстве алгоритмов распознавания мошеннических действий**.

Также в кейсе предлагается к рассмотрению **проблема взаимодействия банка и клиента** в вопросах возврата утерянных денежных средств. Одним из первых действий при совершённых мошеннических операциях является обращение в банк с целью вернуть похищенные средства. Это, единственное, что сделал Антон – и получил отказ в возмещении средств.

Кроме обращения в банк, существуют другие способы получить возврат средств, утраченных из-за мошенников. В качестве альтернативы Антон мог:

А) Написать официальную письменную претензию в адрес банка, затем, в случае получения отказа, обратиться к финансовому уполномоченному.

Б) Попытаться вернуть денежные средства с помощью процедуры chargeback [8].

В) Крайней мерой является судебное разбирательство.

Таким образом, мы считаем, что Антон не до конца использовал возможности, предоставленные законом в части реализации своих прав, однако, исходя из проведённого нами анализа реальных судебных дел, вероятнее всего возврат средств был бы все равно невозможен (см. главу Анализ судебной практики в РФ).

Данная ситуация, на наш взгляд, является парадоксальной и требует подробного анализа изложенной проблематики. Кроме того, наша команда предлагает меры, направленные на контроль за деятельностью ИИ и регулирование взаимоотношений между пользователями финансовых услуг и банками. [30]

Анализ общих проблем и противоречий в применении ИИ.

Перед тем, как анализировать применение искусственного интеллекта в сфере платёжных услуг, мы решили рассмотреть общие проблемы использования и создания ИИ. В результате анализа мы вывели следующие основные проблемы [Приложение 1].

Исходя из полученных данных, можно сделать вывод о том, что на данном этапе развития технологий, многие проблемы являются неразрешимыми, однако есть и те, которые можно преодолеть. Для этого, как мы считаем, необходима правильная регуляция. Сейчас в мире существует множество стратегий развития ИИ, однако ни одна из них не определяет границы данного развития. Таким образом, необходимо учредить некие институты, которые смогут определять и регулировать сферу развития искусственного

интеллекта как в конкретном государстве, так и во всём мире. Так как данный метод несёт за собой большие издержки, а выгоды для конкретного индивида отсутствуют, то создание подобного механизма должно быть возложено на государства мира.

Мировая практика регулирования использования ИИ на рынке платежных услуг

В ходе анализа мировой практики регулирования, мы изучили основные области применения ИИ на рынке платежных услуг (Приложения 2, 3, 4).

В настоящий момент, в мире мало комплексных нормативных актов, относящихся исключительно к ИИ, и нет четкого определения понятия искусственный интеллект. Наиболее близкими к регулированию практики использования ИИ являются:

1. Резолюция Парламента ЕС 2015/2103(INL) от 2017 года, которая касается использования ИИ в робототехнике. [6]
2. «Закон о продвижении разработки и распространения интеллектуальных роботов» в Южной Корее, касающийся роботов, оснащенных ИИ. [7]
3. Закон о защите конфиденциальности потребителей (CPPA) принятый в Канаде 17 ноября 2020 года. [5]
4. Национальные стратегии, в которых содержатся подходы к развитию ИИ, основные проблемы и направления действия.

Однако данные документы являются глобальными и не оказывают непосредственное влияние на регулирование действий искусственного интеллекта.

Сегодня под искусственным интеллектом в основном принято понимать сложные алгоритмы, анализирующие большой объем информации. Источником информации зачастую служат данные пользователей компаний. Соответственно, работа систем, подобных искусственному интеллекту, может регулироваться законами, ограничивающими использование конфиденциальной информации. Такие законы уже существуют в 31 стране, включая Россию. [23]

Примеры предъявления претензий непосредственно к ИИ от пользователей банков оказалось невозможным найти даже в иностранных статьях и сайтах. Для изучения примеров мировой практики регулирования систем искусственного интеллекта в финансовых организациях мы решили выбрать иностранные форумы, на которых люди напрямую заявляют о блокировке их банковских карт или счетов банками. Почему же анализ данного типа источников уместен в работе?

1. Банк блокирует счета, в большинстве случаев используя автоматические системы и алгоритмы, что фактически является искусственным интеллектом на современном этапе развития технологий.

2. На подобное поведение банка обязательно влияет государственная политика, ограничивающая его законами о защите данных и проч.

3. Несмотря на то, что проблема освещается не со стороны регулятора, а со стороны пользователя банковскими услугами, из этой информации вопле возможно понять мотивы регулятора.

Примеры проблемных ситуаций были взяты с форумов: AccountingWEB, Quora, Reddit (Приложение 5).

Примеры иллюстрируют регулирование работы систем безопасности банков как со стороны государства, так и со стороны банка. Можно сделать следующие выводы:

1. При отсутствии регулирования со стороны государства финансовые организации начинают по своей воле вводить ограничения в работу своих систем искусственного интеллекта, так как сталкиваются с проблемами мошенничества и потребностью клиентов в безопасности.

2. Любое регулирование как со стороны банков, так и со стороны государства, обычно приводит к недовольству пользователей, не осознающих необходимость подобных мер во благо безопасности.

3. Введение методов регулирования использования систем искусственного интеллекта – процесс естественный и сам по себе развивается со временем как необходимость, чтобы обеспечивать нормальную работу банков и других финансовых организаций.

Практика регулирования использования ИИ в РФ

ИИ в отечественных банках. Действующие технологии и перспективы. В России, как и во многих других странах, была принята Национальная стратегия развития искусственного интеллекта на период до 2030 г. [2] Её реализация задерживается в условиях пандемии COVID-19, однако её наличие уже говорит о заинтересованности государства, во-первых, в развитии данных технологий на территории России, во-вторых, в желании взять под контроль ситуацию с распространением данных технологий и создать подходящую нормативную базу.

На сегодняшний день лидером по применению решений с использованием ИИ среди банков является Сбербанк. (33, стр. 91) Использование ведется в следующих сферах деятельности: [35, стр. 11]

1. Принятие решений в сфере розничного кредитования (95 % решений принимаются автоматически с использованием систем машинного обучения);

2. При разработке чат-ботов;

3. Моделирование практически всех бизнес процессов в банке с использованием ИИ.

Кроме того, Сбербанк «задает моду» в использовании ИИ другими банками.

Одним из лидеров в области так же является «Тинькофф Банк», специалисты которого утверждают, что ведут разработки в сфере ИИ, не имеющие аналогов не только на отечественном, но даже на зарубежных рынках. [35, стр. 11] К особенностям применения можно отнести:

1. Собственный аналитический сервис AI Research Engine (анализ и предоставление данных для инвестиционных решений).
2. Рекомендательные движки (формирование предложений на основе оценок действий клиента в сети).

Помимо этого, агентство «Эксперт РА» еще в 2018 году оценивало уровень развития ИИ в банках выше среднего по миру в таких банках как: «Газпромбанк» и «МТС Банк». [32]

Исследования KPMG, проведённые в 2019 году, показали, что 72% российских банков в ближайшие годы планируют развивать инструменты ИИ. [36]

Мы провели опрос среди студентов 1-3 курсов на тему использования технологии ИИ в банках. Анализ результатов опроса (Приложение 6) показал, что студенты, в основном, положительно относятся к применению ИИ в сфере безопасности. Это может говорить о том, что эволюция технологий, происходившая в последние годы, улучшила качество услуг. Также большая доля студентов поддерживает введение правового регулирования деятельности ИИ, которое должно привести к улучшению безопасности личных данных.

Политика ЦБ в отношении использования систем искусственного интеллекта. Законодательная база. В реализацию стратегии большой вклад вносит Центральный Банк, который уже использует искусственный интеллект при работе с большими массивами данных и клиентами.

В 2021 году ЦБ опубликовал документ «Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов» [34], в котором, среди прочего, уделяет особое внимание использованию искусственного интеллекта в банковском секторе. Из основных положений в рамках рассматриваемой темы можно выделить:

1. Развитие поведенческого регулирования и надзора за участниками рынка. Планируется применение искусственного интеллекта в поведенческом надзоре для выявления аномалий и зон концентрации поведенческих рисков в деятельности финансовых организаций. [34, стр. 45]
2. Формирование комплексного регулирования оборота данных на финансовом рынке с помощью искусственного интеллекта. [34, стр. 51]
3. Оценка рисков для финансовой стабильности при использовании технологий (искусственного интеллекта и машинного обучения) на финансовом рынке. [34, стр. 67]

Вышеперечисленные положения подтверждают заинтересованность ЦБ в развитии технологий искусственного интеллекта в банковской и финансовой сферах как в области безопасности, так и в качестве инструментов анализа и регулирования рынка.

Так как ЦБ является не законодательным, а исполнительным органом власти, публикуемые им требования имеют рекомендательный характер. Однако, как показывает практика, коммерческие банки активно выполняют требования регулятора.

На данный момент существуют требования ЦБ к безопасности финансовых операций. Анализируемый документ Стандарта Банка России был опубликован в 2020 году. [4] По сути, ЦБ стремится к распространению среди Российских коммерческих банков единых систем, таких как: системы идентификации клиента с использованием технологии защиты OAuth (Приложение 7) и протоколом OpenID Connect (Приложение 8).

Несмотря на высокую скорость разработок и улучшений систем безопасности, ежегодная статистика, публикуемая ЦБ, говорит о ежегодном увеличении объемов операций, выполненных без согласия клиентов (Приложение 9)

Был проведен анализ существующих Российских законов, которые регулируют действие систем искусственного интеллекта на рынке платежных услуг (Приложение 10). Сделаны выводы о влиянии рассмотренных законов на использование СИИ в финансовой сфере.

Анализ судебной практики в РФ. Для анализа существующей судебной практики нами были проанализированы решения кассационных судов. Анализ показал, что суд зачастую встаёт на сторону банков, так как клиенты сами нарушают конфиденциальность своей информации. Случаи перевода без согласия клиента при соблюдении всех норм выполнения операций выявить затруднительно, а возврат денежных средств в большинстве случаев невозможен. В приложение были вынесены случаи, на наш взгляд, типичные для рассматриваемой ситуации. [Приложение 11]

Главная проблема заключается в том, что операции производятся на основе конфиденциальной информации, которая может быть либо украдена у пользователя (например, при введении на стороннем сайте), либо пользователи добровольно сообщают конфиденциальные данные для идентификации и аутентификации в системе банка и дальнейшего использования услуг злоумышленникам.

Таким образом, у банка нет оснований отказать клиенту в услугах в силу норм Гражданского кодекса Российской Федерации, Федерального закона N161-ФЗ [1] и установленных ЦБ России правил осуществления и проверки операций (№ 382-П) [3]. Судебная система, соответственно, встаёт на сторону банка, отказывая в возврате средств

во всех рассмотренных случаях, ссылаясь на подтверждение транзакций через мобильное приложение, смс-уведомление и др.

Также существуют проблемы, связанные с техническими особенностями работы банковских систем. Например, система банка не всегда посчитает операцию как сомнительную даже при многократном отказе её выполнять [14]. Ещё одна проблема – возможность одновременного входа в приложение банка с нескольких устройств [21].

Описание интересов стейкхолдеров, их противоречий и взаимной увязки

Для подробного анализа проблемы необходимо чётко знать, какие стороны имеют свои интересы в применении искусственного интеллекта в сфере платежных услуг, а также понимать, в чём эти интересы заключаются.

1. Регулятор. Несмотря на наличие некоторых выгод от отсутствия регуляционных мер, регулятору (будь то ЦБ РФ или Правительство РФ) будет выгоднее повышение контроля за применением ИИ в платёжной сфере. Это связано с тем, что, как мы считаем, государство более заинтересовано в наличии контроля над рынком, а также в удовлетворённости населения, потому что это куда более осязаемые выгоды.
2. Частные инвесторы. Для частных инвесторов усиление контроля будет означать потерю потенциальных инвестиционных проектов и, как следствие, потенциальной прибыли. Таким образом, инвесторы будут против усиления контроля.
3. Банки и финансовые организации. Как можно понять из Приложения 3, финансовые организации получают достаточно большую прибыль выгоду от разработки ИИ. При нынешних законах банки не испытывают юридических проблем от использования ИИ, поэтому, как мы считаем, будут полностью заинтересованы в отсутствии мер по регулированию данной сферы рынка.
4. Клиенты банков и финансовых организаций. Уже сейчас клиенты банков периодически испытывают неудобства от внедрённых ИИ-технологий. Регулирование данной сферы использования ИИ может избавить клиентов от подобных проблем. Кроме того, мы считаем, что общая регуляция не вызовет недовольство упадком качества сервисов, так как в отсутствие альтернатив многие клиенты не будут осознавать недостатков. Таким образом, клиенты банков будут заинтересованы в повышении уровня регулирования.

Результат анализа интересов стейкхолдеров приведен в Приложении 12.

Возникают очевидные противоречия:

1. Регулятор заинтересован в усилении контроля и в отсутствии финансовых проблем у граждан. Тогда как финансовые организации и инвесторы заинтересованы в ослаблении контроля и их не беспокоят единичные проблемы пользователей.

2. Клиенты банков заинтересованы в повышении контроля, так как это обеспечит уверенность в безопасности средств и персональных данных, а финансовые организации заинтересованы в малом контроле, так как стремятся получить больше выгоды.

Ответы на вопросы

Вопрос 1 Анализ имеющейся информации показал необходимость во введении определенного регулирования использования ИИ на рынке платежных услуг. Меры по контролю должны обязательно:

1. Обеспечивать безопасность клиента во время использования сервисов банка, основанных на технологии искусственного интеллекта;
2. Не быть чрезмерными, то есть ограничивать банки таким образом, чтобы альтернативные способы работы не приносили серьёзных неудобств клиентам.

Таким образом, видится целесообразным введение следующих мер регулирования:

1. Стандартизация классификации «Сомнительные операции», в котором должны быть описаны конкретные условия для признания платёжной операции «сомнительной»;
2. Создание единых стандартов систем искусственного интеллекта, внедряемых в банках.
3. Создание единой системы баз данных систем, включающих статистическую информацию, информацию об ошибках, нарушениях и зарегистрированных случаев мошенничества, нарушителях. Наделение некоторых государственных органов (например, ЦБ) правом доступа к данным.

Предлагаемые нами меры представлены в Приложении 13.

Вопрос 2. Распространение технологии искусственного интеллекта на рынке платёжных услуг влечёт за собой следующие возможности:

1. Повышение безопасности данных клиента. Внедрение технологий с использованием машинного обучение может повысить скорость и качество реагирования банков на кибератаки, которые в данной сфере являются частым явлением. Подобные технологии уже находятся в разработке, что показывает заинтересованность банков в подобных технологиях.
2. Серьёзное снижение затрат банков. Появление технологий на основе искусственного интеллекта в тех сферах банковской деятельности, которые связаны с рутинной, но тщательной проверкой данных, как, например, розничное кредитование, первичное взаимодействие с клиентами и так далее, помогает банкам снизить затраты на функционирование. Это, в свою очередь, убирает необходимость банков в различных

платежах со стороны клиента (так, например, многие современные банки не взимают с пользователей деньги за обслуживание карты).

3. Также использование технологии искусственного интеллекта в сфере платёжных услуг связано с рисками:

- Ошибочная транзакция
- Отсутствие остановки подозрительной транзакции
- Сбой в работе системы – утечка данных, потеря миллионов в случае сбоя из-за остановки работы банка.
- Дальнейшая интеграция подобных технологий может привести к сильной зависимости банков от них, что в свою очередь снижает уровень контроля над своей же системой.

Заключение

На данный момент применение технологии искусственного интеллекта в платёжной сфере влечёт за собой возникновение определённых проблем. Проведённый в ходе работы анализ показал, что на данном этапе отсутствует какое-либо конкретное урегулирование искусственного интеллекта в финансовой сфере на мировом уровне. Несмотря на это, некоторые банки начинают сами вводить меры регуляции, направленные на предотвращение мошеннических операций.

Регулирование технологии ИИ в платёжной сфере в Российской Федерации практически отсутствует. Существует стратегия развития ИИ до 2030 года, и рекомендации ЦБ, а также законы, которые регулируют платёжную сферу, что в данном случае косвенно касается технологии искусственного интеллекта.

В ходе анализа судебных дел кассационных судов субъектов РФ мы выяснили, что все судебные дела решаются в пользу банков, так как клиенты сами нарушают конфиденциальность своей информации.

Список источников

1. Федеральный закон от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/
2. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/44731
3. Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70091962/
4. Стандарт Банка России 2020 СТО БР ФАПИ.СЕК-1.6-2020 [Электронный ресурс]. – Режим доступа: https://cbr.ru/StaticHtml/File/59420/Standart_1.6-2020.pdf
5. BILL C-11. An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts. [Электронный ресурс]. – Режим доступа: https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading
6. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [Электронный ресурс]. – Режим доступа: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
7. Intelligent robots development and distribution promotion act [Электронный ресурс]. – Режим доступа: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=39153&type=lawname&key=robot
8. Правила платежной системы Виза по осуществлению операций на территории Российской Федерации [Электронный ресурс]. – Режим доступа: https://www.visa.com.ru/content/dam/VCOM/regional/cemea/russia/media-kits/documents/VPSORR-31.07.15.pdf
9. Третий кассационный суд общей юрисдикции. Определение от 30 сентября 2021 г. по делу N 88-15836/2021 (Документ предоставлен КонсультантПлюс);
10. Свердловский областной суд. Апелляционное определение от 21 октября 2020 г. по делу N 33-11749/2020 (Документ предоставлен КонсультантПлюс);
11. Четвертый кассационный суд общей юрисдикции. Определение от 26 октября 2021 г. по делу N 88-22791/2021 (Документ предоставлен КонсультантПлюс);

12. Четвертый кассационный суд общей юрисдикции. Определение от 7 сентября 2021 г. по делу N 88-16519/2021 (Документ предоставлен КонсультантПлюс);

13. Четвертый кассационный суд общей юрисдикции. Кассационное определение от 2 июля 2020 г. N 88-14894/2020 (Документ предоставлен КонсультантПлюс);

14. Второй кассационный суд общей юрисдикции. Определение от 23 октября 2020 г. по делу N 88-21454/2020 (Документ предоставлен КонсультантПлюс);

15. Второй кассационный суд общей юрисдикции. Определение от 26 октября 2021 г. N 88-23370/2021 (Документ предоставлен КонсультантПлюс);

16. Второй кассационный суд общей юрисдикции Определение от 14 декабря 2021 года N 2-665/2021 (Документ предоставлен КонсультантПлюс);

17. Восьмой кассационный суд общей юрисдикции. Определение от 24 марта 2021 г. по делу N 88-4223/2021(8г-543/2021) (Документ предоставлен КонсультантПлюс);

18. Восьмой кассационный суд общей юрисдикции. Определение от 25 августа 2021 г. N 88-14574/2021 (Документ предоставлен КонсультантПлюс);

19. Восьмой кассационный суд общей юрисдикции. Определение от 6 октября 2021 г. N 88-16818/2021(8г-18174/2021) (Документ предоставлен КонсультантПлюс);

20. Седьмой кассационный суд общей юрисдикции. Определение от 20 января 2020 г. N 88-644/2020 (Документ предоставлен КонсультантПлюс);

21. Седьмой кассационный суд общей юрисдикции Определение от 3 ноября 2021 г. N 88-16938/2021 (Документ предоставлен КонсультантПлюс);

22. AI for Cybersecurity in Finance – Current Applications. [Электронный ресурс]. – Режим доступа: https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/

23. Artificial Intelligence Law: Discover How the Law Applies to AI [Электронный ресурс]. – Режим доступа: https://www.rev.com/blog/artificial-intelligence-law-how-the-law-applies-to-ai

24. Bank Acct frozen...bank not explaining [Электронный ресурс]. – Режим доступа: https://www.accountingweb.co.uk/any-answers/bank-acct-frozenbank-not-explaining

25. Carbon Emissions and Large Neural Network Training [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2104.10350

26. Cybersecurity M&A volume reaches $77.5 billion in 2021 [Электронный ресурс]. – Режим доступа: https://www.zdnet.com/article/cybersecurity-m-a-volume-reaches-77-5-billion-in-2021/

27. My Bank of America app tells me that my account is locked? What does that mean? [Электронный ресурс]. – Режим доступа: https://www.quora.com/My-Bank-of-America-app-tells-me-that-my-account-is-locked-What-does-that-mean

28. One of the World's Largest Investment Management Firms Signs Major Contract with Darktrace [Электронный ресурс]. – Режим доступа: https://www.darktrace.com/en/press/2021/380/

29. TD Bank blocking crypto purchases [Электронный ресурс]. – Режим доступа: https://www.reddit.com/r/CryptoCurrency/comments/7mn611/canada_td_bank_blocking_crypto_purchases_because/

30. The impact of artificial intelligence in the banking sector & how AI is being used in 2022. [Электронный ресурс]. – Режим доступа: https://www.businessinsider.com/the-ai-in-banking-report-2019-6

31. Антифрод-системы нового поколения – искусственный интеллект против мошенников [Электронный ресурс]. – Режим доступа: https://plusworld.ru/journal/section_1817/plus-10-2017/antifrod-sistemy-novogo-pokoleniya-iskusstvennyj-intellekt-protiv-moshennikov/

32. Искусственный интеллект в банковском секторе [Электронный ресурс]. – Режим доступа: https://www.raexpert.ru/researches/banks/bank_ai2018/

33. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс]. – Режим доступа: https://cbr.ru/analytics/ib/review_3q_2020/

34. Основные направления развития финансового рынка российской федерации на 2022 год и период 2023 и 2024 годов [Электронный ресурс]. – Режим доступа: https://cbr.ru/Content/Document/File/131935/onrfr_2021-12-24.pdf

35. Семеко Г. В. «Искусственный интеллект в банковском секторе: возможности и проблемы» // Социальные новации и социальные науки. – Москва : ИНИОН РАН, 2021. – № 2. – С. 81–97. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-bankovskom-sektore-vozmozhnosti-i-problemy

36. Цифровые технологии в российских компаниях [Электронный ресурс]. – Режим доступа: https://home.kpmg/ru/ru/home/insights/2019/01/digital-technologies-in-russian-companies-survey.html

37. Research in the Crowdsourcing Age, a Case Study [Электронный ресурс]. – Режим доступа: https://www.pewresearch.org/internet/2016/07/11/research-in-the-crowdsourcing-age-a-case-study/

Приложение 1

Таблица 1. Проблемы, связанные с использованием ИИ

Название проблемы	**Суть проблемы**	**Возможное решение**
Проблемы определения термина «ИИ»	В настоящее время не существует единого определения искусственному интеллекту. Кто-то определяет его, как машину, имитирующую человеческое поведение, а кто-то как систему, способную делать выводы и принимать решения без участия человека. Учёные не достигли консенсуса по данному вопросу.	Потенциальным решением проблемы является определение всех типов искусственного интеллекта и последующая их классификация.
Юридический статус ИИ	На данном этапе искусственный интеллект является лишь собственностью компании, однако в будущем возможно становление ИИ, который будет подобен человеку. Потому многие учёные спорят о том, стоит ли признать ИИ равным человеку, или же нет.	Если в процессе разработки ИИ, а также инструментов с его участием, не дать искусственному интеллекту пересечь ту черту, которая отделяет его от человека, то есть не наделить его человеческими чувствами и эмоциями, то полученный в результате ИИ априори не будет рассматриваться как нечто равное человеку. Для достижения подобных результатов, необходима правильная регуляция со стороны государств мира.
Проблема базы данных ИИ	Для обучения ИИ используются определённые базы данных, однако они априори неполные. Потому ИИ, анализируя выборку, может прийти к неправильному выводу.	Данная проблема не может быть решена. Сбор базы данных всегда будет сопряжен с отбором информации, что оставляет возможность для появления ошибок.
Трудоёмкое «обучение» ИИ	Для того, чтобы искусственный интеллект обучался, ему требуется огромное количество информации. Сбор этой информации не осуществим без участия людей. Существуют некоторые сервисы, на которых люди участвуют в сборе информации, однако это не является достаточным. Кроме того, по данным исследовательского центра “Pew” данная работа низкооплачиваемая. Больше половины работников таких сервисов получают меньше 5 долларов в час, что меньше минимальной зарплаты в США. [37]	В нынешнее время решение данной проблемы невозможно, так как с подобной работой способен справиться лишь человек.

Продолжение Таблицы 1

Машинное обучение работает отлично от человеческого мозга	Человеку одновременно трудно и легко понять искусственный интеллект. Простые разработки ИИ легко обмануть, а сложные порой невозможно понять. Таким образом, можно поставить под сомнение целесообразность использования данных технологий.	Решение данной проблемы находится в создании базы данных, которая поможет находить общие проблемы, а также бороться с непрозрачностью алгоритмов некоторых ИИ
Технологическая безработица	Новые разработки в сфере технологии искусственного интеллекта влекут за собой автоматизацию механических процессов, которые раньше выполнялись людьми (к примеру, интернет-консультанты). Это неизменно влечет за собой появление технологической безработицы.	Государства в состоянии бороться с безработицей. Например, можно позаботиться о создании определённых институтов, которые помогут в перепрофилировании безработных граждан. Если же безработица будет слишком велика, то можно ввести определённые социальные гарантии.
Вред экологии	Обучение и работа ИИ потребляет огромная количество энергии. Например, согласно работе исследователей из Беркли, самая продвинутая языковая модель GPT-3 за год обучения выработала 552 метрических тонн углекислого газа, что эквивалентно вождению 120 легковых автомобилей целый год. [25]	Данную проблему возможно нивелировать переходом систем искусственного интеллекта на возобновляемые источники энергии.

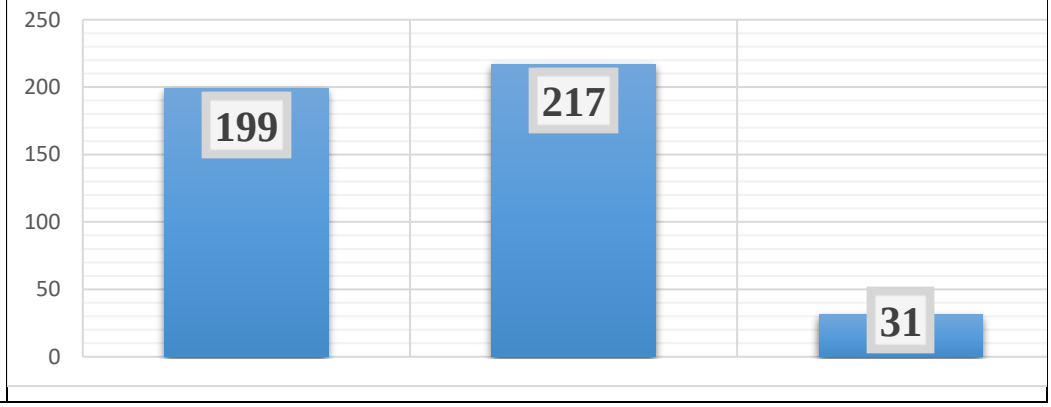
Приложение 2

Таблица 2. Анализ мировой практики применения ИИ на рынке платежных услуг

Основные выгоды от использования ИИ	
1. Снижение затрат	По оценкам экспертов, за счет использования ИИ, в период с 2019-2022 год в мировом финансовом секторе удалось сэкономить 447 млрд долларов США (Таблица 3)
2. Защита от кибератак	Необходимость у банков в обеспечении защиты своих информационных инфраструктур способствует развитию рынка программных решений в области искусственного интеллекта. Существуют реальные примеры положительных результатов действия систем искусственного интеллекта в работе банков в период с 2019 года (Таблица 4)
3. Привлечение и удержание клиентов	Привлечение и удержание клиентов. Системы искусственного интеллекта также активно применяются при разработке голосовых ассистентов, которые значительно упрощают процесс взаимодействия клиента с сервисами банка. Цели использования чат-ботов банками: ● Привлечение новых клиентов ● Автоматизированная поддержка часто задаваемых вопросов ● Уведомления и напоминания ● Активная коммуникация с клиентами ● Помощь в финансовых консультациях ● Мониторинг счетов ● Обработка платежей ● Предотвращение мошенничества ● Сбор отзывов клиентов

Приложение 3

Таблица 3. Общая экономия в банковском секторе от использования ИИ [30]

Использование ИИ в банковской сфере			
Подразделения	Фронт-офис	Мидл-офис	Бэк-офис
Основные области использования	Взаимодействие с клиентом; Биометрия	Борьба с мошенничеством; Оценка рисков	Оформление кредитов; Работа с документами
Общие объемы экономии, млрд. долл.			

Приложение 4

Таблица 4. Примеры использования систем киберзащиты в работе банков и финансовых организаций [22],[28]

Производители программного обеспечения для компаний	**Область применения решений**	**Крупнейшие клиенты**	**Результаты использования финансовыми организациями**
Feedzai	- Обнаружение мошенничества; - Препятствование отмыванию денег; - Снижение кол-ва ложных срабатываний; - Ускорение принятия заявок на проведение транзакций.	- Capital One - City	Увеличение количества заявок в среднем на 70% за аналогичный временной период
DefenseStorm	- Мониторинг внутренних систем; - Поиск аномалий в сети в режиме реального времени.	- Live Oak Bank - Washington Trust Bank	- Live Oak Bank смог оптимизировать поиск больших данных и повысил обнаружение инцидентов на 50-60%; Интеграция платформы - DefenseStorm снижает время анализа проблемной ситуации до 1 мин. (в ручном режиме требовалось 15-20 мин.)

Продолжение таблицы 4

Darktrace	- обнаружение и реагирование на киберугрозы с использованием машинного обучения - защита таких объектов, как облако, виртуальные сети, промышленные системы управления	- фирмы по управлению инвестициями [26]; - компании, занимающиеся информационной аналитикой; - некоторые государственные органы в США - Birmingham Airport	- рекордная скорость реакции на киберугрозы; - получение 3д визуализации процессов, происходящих в сети компании
PatternEx	- идентификация намерений злоумышленника; - прогноз и предотвращение кибератак	нет информации	нет информации

Приложение 5

Таблица 5. Примеры проблемных ситуаций, взятых с форумов

Проблема, рассматриваемая на форуме	Причины проблемы, исходя из ответов на форуме	Выводы
1. Счет в банке заблокирован. Банк не раскрывает причин. [24]	На основании ряда законов, таких как Proceeds of Crime Act 2002 (POCA), Money Laundering Regulations 2007 (MLR), порог подозрения в мошеннических сделках очень низок; Банки имеют очень чувствительную систему и фактически могут заблокировать транзакцию и счет без объяснения причин.	Данный пример иллюстрирует последствия чрезмерно жесткого регулирования и наблюдения за деятельностью банков ради обеспечения высокого уровня безопасности. При этом у клиентов банка вместо недовольства от угрозы мошенничества возникает недовольство от неудобства банковских сервисов.
2. Bank of America заблокировал счет после перевода средств на счет в другом онлайн банке. [27]	Банк Америки изменил свою политику безопасности, согласно которой он блокирует счета, с которых совершаются попытки переводов на счета онлайн - банков, то есть банков, не имеющих физических филиалов. Банк плохо уведомляет клиентов об изменении правил, и они вынуждены обращаться за юридической помощью, чтобы разобраться в ситуации.	При отсутствии регулирования банковских информационных систем законами, банк начинает сам регулировать их деятельность, поскольку несет большие издержки от мошенничества и различных махинаций.
3. Канадский TD Bank блокирует переводы в криптовалюте. [29]	TD Bank вводит в действие политику, которая блокирует доступ пользователей Северной Америки к операциям с криптовалютой за пределами своего континента.	

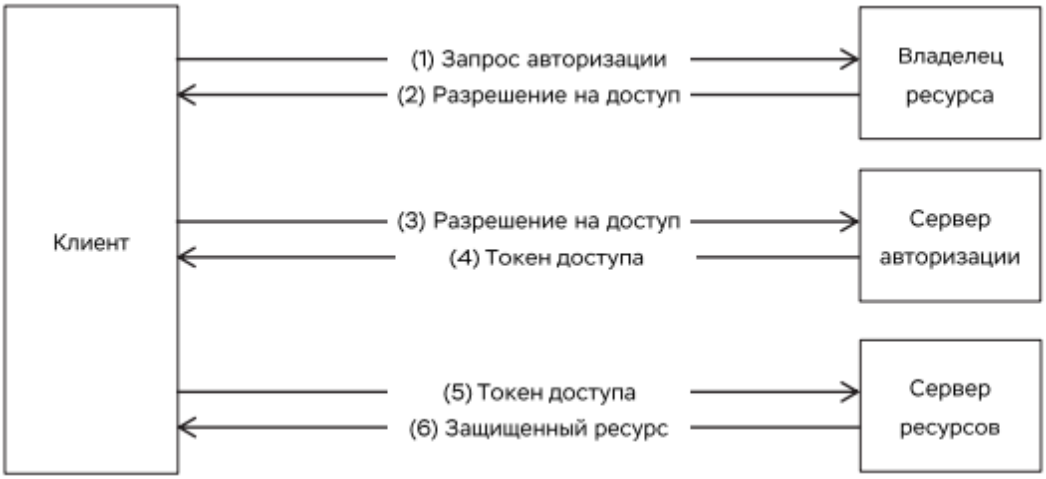
Приложение 6

Таблица 6. Опрос студентов

Вопрос	**Ответ**	**Краткий анализ**
На каком курсе вы учитесь?	1-14(20%) 2-14(20%) 3- 37(52,9%) 4- 5(7,1%)	Всего опрошено 70 человек
Имеете ли вы счет в банке?	Да – 57 (81,4%) Нет – 13 (18,6%)	Большая часть опрошенных имеет счёт в банке, открытый для получения стипендиальных выплат
Клиентом какого банка вы являетесь? (вопрос с множественным выбором)	Сбер – 69 (98,6%) Альфа-банк -5(7,1%) Тинькофф - 18 (25,7 %) ВТБ-7(10%) Газпромбанк- 1 (1,4%) Почтабанк – 1 (1,4%) Росбанк – 2 (2,8%)	Высочайший процент пользователей Сбера является следствием получения стипендиальных выплат на карты этого банка. Также, довольно высокой популярностью среди студентов пользуется банк Тинькофф.
Сталкивались ли Вы с неправомерным списанием (попыткой неправомерного списания) средств со счета?	Да, лично пострадал- 3(4,3%) Да, лично знаю пострадавших – 12(17,1%) Нет, не сталкивался, но слышал, что такое может произойти - 53(75,7%) Нет, не сталкивался и не думаю, что это возможно – 2(2,9%)	В сумме 21,4% опрошенных сталкивались с незаконным списанием средств лично либо знакомы с пострадавшими, что является очень весомым показателем активности мошенников
Считаете ли вы систему защиты банковских платежей вашего банка достаточной?	Да – 46 (65,7%) Нет – 19(34,3%)	Лишь 65,7% опрошенных считают защиту банковских платежей своего банка достаточной. Это может быть связано с сильно возросшим количеством незаконных списаний средств с банковских счетов.
Как вы считаете, уместно ли использовать системы искусственного интеллекта в обеспечении безопасности расчетов и платежей?	Да – 51 (72,9%) Нет – 19(27,1%)	72,9% опрошенных считают уместным использование ИИ в обеспечении безопасности расчётов. Основной причиной такого высокого результата может являться возрастная категория опрошенных.
Доверяете ли вы банку при использовании им ваших персональных данных?	Да - 47(67,1%) Нет – 23(32,9%)	Основной причиной недоверия к банкам в случаях использования персональных данных являются массовые утечки, публикуемые в сети Интернет
Считаете ли вы, что государство должно жестче регулировать использование банками новых технологий, связанных с искусственным интеллектом?	Да – 58 (82,9%) Нет – 12 (17,1%)	Высокий процент, выступающих за усиление контроля над ИИ, обусловлен фактическим отсутствием нормативной базы по контролю и регулированию деятельности ИИ
Вы положительно относитесь к применению ИИ в обыденной жизни человека?	Да – 58 (82,9%) Нет – 12 (17,1%)	Положительное отношение к ИИ в обыденной жизни связано с значительным упрощением ежедневных операций в случае интеграции ИИ
Используете ли Вы сервисы банка, которые основаны на применении ИИ (например, "Салют" от Сбера)?	Нет – 48(68,6%) Да, довольно часто – 3(4,3%) Да, иногда -8 (11,4%) Да, очень редко (пользовался/ась один раз) – 11(15,7%)	Низкий процент использования сервисов банка, основанных на ИИ, обусловлен узким функционалом и невысоким качеством продуктов

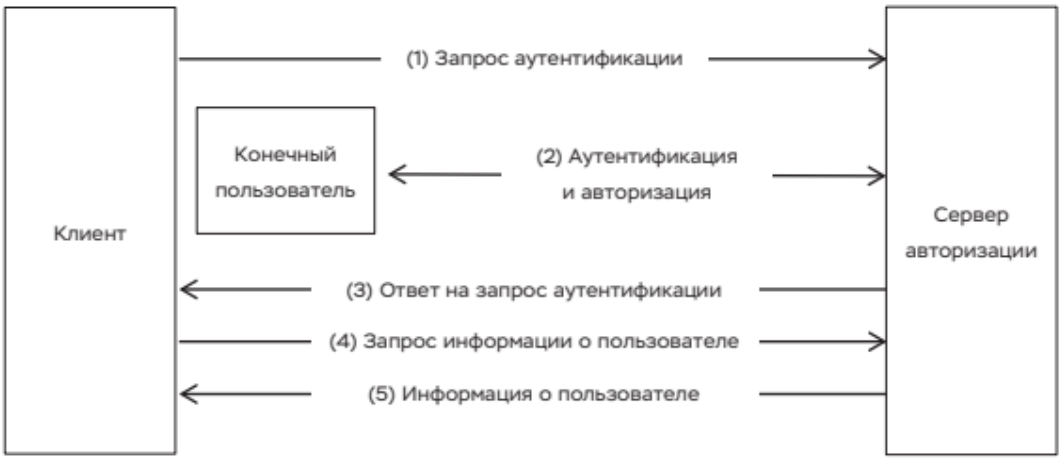
Приложение 7

Рисунок 1. Сценарий протокола OAuth 2.0 [4]



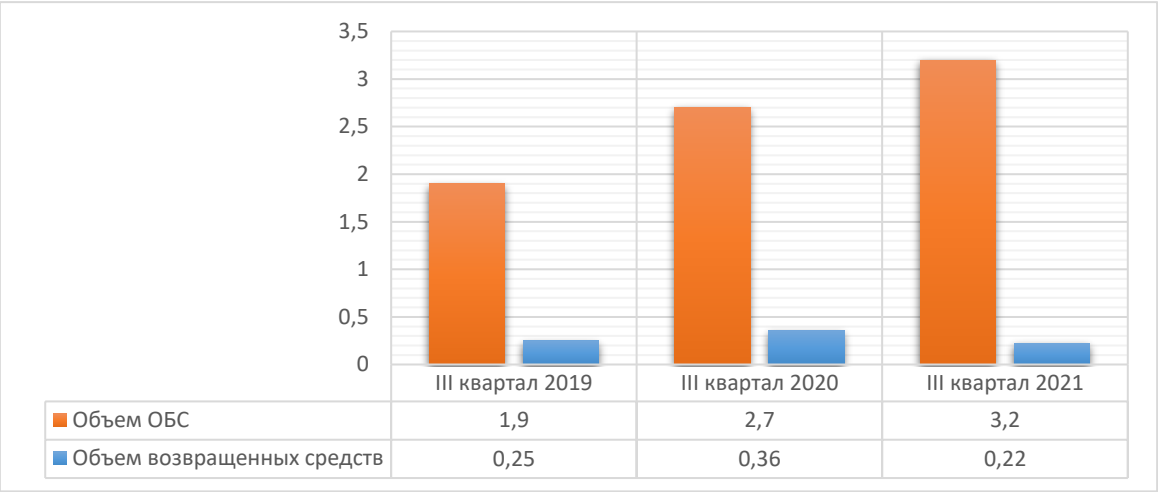
Приложение 8

Рисунок 2. Сценарий аутентификации OpenID Connect [4]



Приложение 9

Рисунок 3. Объем ОБС (операций без согласия клиента) за III квартал 2019-2021гг, млрд. руб. Источник: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [33]



Приложение 10

Таблица 7. Анализ законодательного регулирования использования систем искусственного интеллекта

Законы	Меры, которые могут касаться использования ИИ	Влияние на использование СИИ в финансовой сфере
ФЗ "О национальной платежной системе" от 27.06.2011 N 161-ФЗ	• Требования к организации и функционированию платежных систем; • Регулирование порядка использования электронных средств платежа; • Обеспечение защиты информации, банковской тайны;	Определение основных правил функционирования и взаимодействия операторов по переводу денежных средств. Соответственно деятельность ИИ в сфере платежных услуг должна соответствовать требованиям данного закона.
ГК РФ, Глава 45. Банковский счет.	• Определение ответственности банка за ненадлежащее совершение операций по банковскому счету;	Определяет ответственность банка или финансовой организации за нарушения в следствие действий ИИ.
"Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ	• Регулирует осуществлении права на поиск, получение, передачу, производство и распространение информации; • Обеспечение защиты информации	Ограничивает системы искусственного интеллекта в использовании информации о клиентах (к примеру, использование персональных данных в работе рекомендательных движков).
"О персональных данных" от 27.07.2006 N 152-ФЗ	• Определяет правила сбора, систематизации, накопления, использования персональных данных (в том числе с использованием автоматизированных систем).	
"О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" от 19.12.2005 N 160-ФЗ		

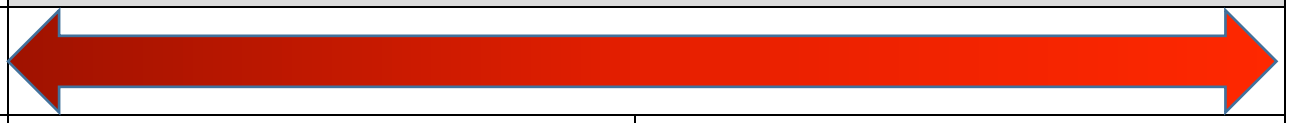
Приложение 11

Таблица 8. Анализ примеров судебной практики в РФ. Определения кассационных судов, судов субъектов РФ, типичные примеры.

Дело	**Описание**	**В чью пользу вынесено решение.**
Седьмой кассационный суд общей юрисдикции. Определение от 3 ноября 2021 г. N 88-16938/2021 [21]	Истец утверждал, что **неизвестные вошли в систему «ВТБ-онлайн» и совершили операцию без его согласия**, однако суд установил ,что для входа был использован смс-код отправленный на привязанный номер телефона, в связи с чем совершенный перевод не имел признаков осуществления перевода денежных средств без согласия и списание денежных средств со счета истца осуществлялись в полном соответствии с условиями договора комплексного обслуживания посредством ввода Passcode (система авторизации ВТБ), в связи с чем у банка не имелось оснований для приостановления исполнения распоряжения о совершении операции. Вследствие этого суд отказал истцу с удовлетворением иска о возврате денежных средств.	Банк
Второй кассационный суд общей юрисдикции. Определение от 23 октября 2020 г. по делу N 88-21454/2020 [14]	Истец утверждал, что ему **позвонили сотрудниками банка. В результате разговора он сообщил им свои конфиденциальные данные, а также смс-коды, приходившие ему 9 раз подряд**. **Восемь раз операция была отклонена, но на девятый раз система разрешила проведение операции**. Истец утверждает, что при многократной попытке совершить операцию банк должен был заморозить проведение операции, но не сделал этого, в связи с чем банк должен выплатить ему компенсацию. Однако суд постановил, что банк не может быть признан виновным в неисполнении своих обязанностей, поскольку клиентом были выполнены все необходимые процедуры для того, чтобы считать снятие средств правомерным, так как каждая операция была подтверждена высланным на мобильное устройство истца соответствующим кодом, полученным и использованным истцом.	Банк
Свердловский областной суд. Апелляционное определение от 21 октября 2020 г. по делу N 33-11749/2020 [10]	**Суд установил, что истец сообщила неустановленному лицу данные карты, трехзначный код, а также секретные коды из смс-сообщений, что исключает ответственность банка за последующее списание средств** и оформление кредитного договора, так как банком была проведена проверка операций, которые отвечали критериям, установленным Центральным банком Российской Федерации. Так же было указано, что безотзывность переводов наступила в момент проведения спорных операций. Решением суда исковые требования оставлены без удовлетворения.	Банк

Приложение 12

Таблица 9. Анализ интересов стейкхолдеров

	Государственное регулирование и контроль	
		
	Слабее	**Сильнее**
	Цели: • Дать возможность бизнесу быстрее осваивать новые технологии в сфере ИИ • Повышение инициативы собственных разработок СИИ отечественными банками. • Улучшение качества услуг банков и фин. организаций, в случае если государственное вмешательство пагубно влияет на качество сервисов (тратятся ресурсы на слежение, снижается скорость работы сервисов).	***Цели:*** • Снижение рисков мошенничества в интересах клиентов • Развитие законодательной базы в процессе практики регулирования использования банками СИИ, которое пригодится и в других сферах деятельности в будущем. • Сбор статистических данных и контроль над информацией об использовании СИИ в финансовой сфере.
	Регулятор	
Выгоды	• Уменьшение издержек на реализацию различных мер контроля. • Свобода на рынке технологий повышает конкурентность и, как следствие, качество услуг.	• Усиление общего контроля над рынком платёжных услуг. • Возможность получения информации о конкретных технологиях, используемых банками.
Проблемы	• Риск возникновения сильной негативной реакции населения на новую технологию, внедрённую банком. • Проблемы в юридической сфере из-за трудно решаемых судебных разбирательств.	• Увеличение издержек на использование соответствующих мер контроля. • Риск возникновения недовольства банков и финансовых организаций по поводу жёсткого регулирования рынка.
	Частные инвесторы	
Выгоды	• Возможность свободно инвестировать в любые технологии, не опасаясь потерять вложения из-за политики регулятора. • Отсутствие регуляции увеличивает количество потенциально прибыльных инвестиционных проектов.	• Снижение риска инвестирования в технологию, способную вызвать крупное недовольство у клиентов банка. •

Продолжение Таблицы 9

Проблемы	• Присутствие на рынке мошенников	• Уменьшение количества технологий, в которые можно выгодно инвестировать капитал.
	Банки и финансовые организации	
Выгоды	• Свобода в выборе/разработке СИИ, направлениях их использования; • Внедрение ИИ для улучшения качества оказываемых услуг (привлечение и удержание клиентов); • Использование ИИ для внутренней работы банковских систем (снижение расходов, экономия времени); • Возможность свободного использования зарубежного опыта в работе с ИИ.	• Четкое нормативное описание правил использования СИИ и стандартизация, снижают количество конфликтных ситуаций, судебных дел; • Снижение случаев мошенничества при пользовании банковскими сервисами.
Проблемы	• Повышение рисков мошенничества и других операций, не желательных для банка и для клиента; • Свобода в выборе инструментов, связанных с ИИ, может привезти к зависимости отечественных банков от иностранных технологий.	• Ограничения тормозят процесс внедрения технологий; • Риск ухудшения работы сервисов за счет дополнительного сбора информации и формирования отчетов; • Дополнительные затраты, связанные с подстраиваем систем под нормы права.
	Клиенты банков и финансовых организаций (физ. и юр. лица)	
Выгоды	• Постоянно повышается количество и удобство новых сервисов;	• Уверенность в безопасности для средств и информации при использовании сервисов; • Уверенность в стабильности работы банковских сервисов
Проблемы	• Недоверие к банкам по вопросам использования конфиденциальной информации; • Увеличение рисков мошенничества.	• Дополнительные проверки действий при пользовании сервисами банков; • Использование государством персональных данных клиентов • Возможное неудовлетворение работой сервисов (становятся медленнее, чаще отклоняются платежи).

Приложение 13

Таблица 10. Предлагаемые меры

Предлагаемая мера	Преимущества	Недостатки	Сторонники	Противники
1. Разработка единых обязательных стандартов систем искусственного интеллекта	• Повышение безопасности систем, уменьшение риска мошеннических операций. • Стандартизация процесса обмена информации.	• Замедление развития новых технологий • Отсутствие свободы выбора во внедрении новых систем • Затраты на переход к использованию стандартов	**Клиенты:** повышение уровня безопасности, возможное снижение скорости обслуживания **ЦБ:** Повышение качества работы и безопасности финансовой системы	**Банки:** Увеличение издержек на дополнительные проверки операций, возможное снижение скорости систем **Инвесторы:** возможное уменьшение прибыли от вложения в банковские организации
2. Формирование правовой основы регулирования ИИ	• Улучшение обеспечении защиты данных граждан и бизнеса • Улучшение кибербезопасности и киберустойчивости элементов национальной платежной системы России.	• Замедление развитие технологий. • Возможность чрезмерного регулирования, в результате снижение скорости работы систем	**Клиенты:** повышение уровня безопасности, возможное снижение скорости обслуживания **ЦБ:** Повышение качества работы и безопасности финансовой системы **Инвесторы:** возможность вложить средства в технологии, которые будут сразу соответствовать нормам права, а значит иметь меньше риска	**Банки:** издержки на подстраивание систем под нормы права

Продолжение таблицы 10

3. Создание единой базы данных поиска и отслеживания мошеннических операций.	• Повышение безопасности операций • Увеличение скорости выявления и корректировки отклонений в транзакциях	• Снижение скорости выполнения операций, а также возможность снижения безопасности конфиденциальных данных ввиду усложнения систем	**Клиенты:** повышение уровня безопасности. **ЦБ:** Улучшение безопасности финансовой системы	**Банки:** повышение издержек на проведение операций, снижение скорости работы систем
4. Создание сертифицированных ЦБ систем и технологий в области искусственного интеллекта придерживаясь концепции открытого программного обеспечения (Open Source)	• Снижение издержек, возможность большему числу финансовых организаций использовать продвинутые технологии в обслуживании. • Повышение безопасности операций, гарантии безопасности конфиденциальных данных, так как любой сможет проверить что система не распространяет эти данные.	• Замедление развития новых технологий. • Увеличение влияния крупных игроков на рынке, в силу обладания большими финансовыми возможностями для разработки и внедрения эксклюзивного программного обеспечения.	**Клиенты:** Расширенная возможность выбора организаций для обслуживания, использующих продвинутые технологии **ЦБ:** Повышение уровня безопасности	**Банки:** Возможные слишком высокие издержки на поддержание подобных систем. Большая выгода в использовании готовых сторонних систем. **Инвесторы:** возможное уменьшение прибыли от вложения в банковские организации
5. Введение обязательной нормы возврата средств в	• Упрощённый порядок возврата	• Усложнение систем, снижение скорости	**Клиенты:** Гарантированная	**Банки:** увеличение издержек и рисков.

случае выявлении мошенничества	похищенных средств, зависящий от уровня технологий противодействия мошенническим операциям, используемых в банках.	операций, так как возрастает количество проверок при проведении операций. • Возможность злоупотребления нормой со стороны недобросовестных клиентов.	возможность вернуть потерянные средства **ЦБ:** Повышение уровня доверия к финансовой системе	**Инвесторы:** уменьшение прибыли в организациях, в которые были сделаны вложения