СЕВЕРО-ЗАПАДНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ

Команда «СПбГЭУ»

Аналитическая записка

Искусственный интеллект, большие данные и безопасность расчетов и платежей

Авторы:

Грачева Руслана Эдуардовна: ruslana.gracheva@mail.ru, СПбГЭУ

Гуценко Павел Романович: kg12072000@gmail.com, СПбГЭУ

Дерняева Анна Сергеевна: 11.05@list.ru, СПбГЭУ

Паневина Юлия Сергеевна: panevinay@mail.ru, СПбГЭУ

Преподаватель-тренер:

к.э.н. доц. Петрова Наталья Павловна: natashanpk@yandex.ru, Petrova.n@unecon.ru

Санкт-Петербургский государственный экономический университет

Кафедра финансов

Санкт-Петербург

2022

Введение

Цифровая трансформация (digital transformation) определяет вектор развития как национальной экономики, так и корпоративного сектора. Позиция государства в этом вопросе была обозначена Указом Президента РФ от 7 мая 2018 г. №204 «О национальных целях и стратегических задачах развития РФ на период до 2024 года». В 2020 году горизонт планирования был продлен до 2030 года.[1] Данный проект направлен на поддержку и развитие государственного управления, новых технологий, информационной безопасности, искусственного интеллекта (ИИ).

Организация экономического сотрудничества и развития (OECD) под цифровой трансформацией понимает «совокупность экономических и социальных эффектов в результате цифровизации; использование данных и цифровых технологий для создания новых или изменения существующих видов деятельности».[2] Авторы работы разделяют данную позицию и считают, что цифровая трансформация кроме технологических решений предполагает перестройку бизнес-процессов с целью оптимизации.

По оценкам Национального исследовательского университета высшей школы экономики «валовые внутренние затраты на развитие цифровой экономики в 2019 г. составили 4,1 трлн руб. и достигли 3,7% ВВП. Расходы организаций на приобретение, монтаж и ввод в эксплуатацию оборудования, связанного с цифровыми технологиями, в 2019 г. достигли 1088,6 млрд руб.» [3], из них 53,5% на закупку вычислительной техники; около 30,9% – на коммуникационное оборудование и 3,7% – на производственные машины и оборудование. В «структуре внутренних затрат организаций на создание, распространение и использование цифровых технологий по видам экономической деятельности лидируют телекоммуникационные компании - 21,6%, организации, чья деятельность связана с научной и технической сферой -19,7% и финансовые и страховые компании -15,5%».[4]

Центральный банк РФ как мегарегулятор поддерживает цифровизацию финансового рынка. Так, в 2016 году по его инициативе была открыта Ассоциация «ФинТех», деятельность которой направлена на создание условий для цифровизации экономики РФ и внедрение новых технических решений на финансовом рынке. Также Банк России является уполномоченным органом в сфере экспериментальных правовых режимов по направлению

---

[1] Указ Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» http://www.consultant.ru/document/cons_doc_LAW_357927/

[2] OECD (2019). Science and Technology vectors of Digital Transformation: https://www.oecd-ilibrary.org

[3] Доклад НИУ ВШЭ Цифровая трансформация отраслей: стартовые условия и приоритеты https://conf.hse.ru/mirror/pubs/share/463148459.pdf.

[4] Доклад НИУ ВШЭ Цифровая трансформация отраслей: стартовые условия и приоритеты https://conf.hse.ru/mirror/pubs/share/463148459.pdf.

«финансовый рынок».[5] Основные проекты банка на 2022-2024 г. связаны с развитием системы быстрых платежей, цифрового профиля, цифрового рубля, единой биометрической системой, платформы коммерческих согласий, цифровизацией ипотеки и исполнительного производства. Кроме того, мегарегулятор уделяет большое значение развитию финансовой безопасности. В 2015 году в ЦБ был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России). Ассоциация банков России с 2018 года внедряет платформу для обмена данными между кредитными организациями по вопросам кибератак.

Пандемия COVID-19 способствовала развитию цифровизации, дистанционных услуг и безналичных расчетов. За 2020-2022 гг. использование дистанционных услуг в мире увеличилось на 23%, а мобильных банковских приложений – на 30%. Так по данным Центрального банка (ЦБ) в 2020 году доля граждан, которые предпочитают использовать безналичную форму оплаты для расчетов составила 70%[6] (см. Приложение 1). На 01.10.2021 г. было открыто 293 419,9 тыс. счетов в кредитных организациях с дистанционным доступом, что составляет 30% от общего числа счетов, открытых учреждениями банковской системы (см. Приложение 2).

Аналитики HIS Markit отмечают, что в 2018 году банки заработали около 41 млрд долл. с помощью ИИ, к 2030 году этот показатель может достичь 300 млрд долл. Опрос компании OpenText показывает, что 80% банков осознают выгоду использования ИИ в своей деятельности.[7] По оценкам экспертов, в 2021 году банки потратили на эти цели более 217 млрд. долл.[8] В финансовых организациях ИИ способствует сокращению расходов, повышению доходов, улучшению клиентского опыта, автоматизирует внутренние процессы, позволяет ускорить процессы идентификации и аутенфикации. Одной из главных целей ИИ в финансовом секторе является выявление мошеннических операций. По данным ЦБ только с апреля по июнь 2021 года мошенники украли 3 млрд рублей у клиентов российских банков – в 1,5 раза больше, чем годом ранее (см. Приложение 3). Для предотвращения мошеннических транзакций банки используют антифрод системы. ИИ формирует шаблоны, основанные на исторических данных о поведении пользователей, и таким образом строит прогнозы. Таким образом, использование современных цифровых технологий, ИИ и больших данных является актуальным. Цель исследования заключается в определении влияния искусственного интеллекта на безопасность расчетов и платежей.

---

[5] Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31.07.2020 № 258-ФЗ: http://www.consultant.ru

[6] Статистика национальной платежной системы https://cbr.ru/statistics/nps/psrf/

[7] Исследование: крупные банки чаще используют искусственный интеллект https://frankrg.com/12651

[8] Как устроен антифрод и почему с мошенниками так сложно бороться https://trends.rbc.ru/trends/industry/6167ff259a7947f4c6908e46

Основная часть

Для лучшего понимания темы ИИ, больших данных и безопасности расчетов и платежей необходимо проанализировать данные кейса.

Из задания видно, что Антону как студенту технического вуза не хватило личных знаний в вопросах управления и безопасности финансов. При выборе банка он ориентировался на IT-технологии и не учёл, что любой вопрос, связанный с денежными средствами, нужно контролировать самостоятельно. Первая ошибка была совершена Антоном уже при приобретении билетов. Однозначно студент стал жертвой интернет-мошенничества, на его компьютер произошла фишинговая атака. Он, желая попасть на концерт, перешел на «зеркальный/поддельный» сайт и совершил там покупку. Возможно, мошенники уже заранее собирали данные о его предпочтениях по поисковым запросам с помощью приемов социальной инженерии, и, возможно, переход на фишинговый сайт произошел не случайно. Скорее всего устройство, с которого он заходил на сайт, не имело лицензионного антивирусного программного обеспечения, которое бы распознало атаку.

Антон при переходе на сайт продавца, возможно, не обратил внимание на адресную строку. Официальный сайт должен начинаться с букв https и иметь символ замка. Уже на этом этапе Антон скомпрометировал данные своей карты, и мошенники получили к ней доступ. Студент при управлении своими финансами игнорирует вопросы эффективности и минимизации рисков. Он держит все свои сбережения на одной банковской карте. Ему следует диверсифицировать свои активы, распределив денежные средства по нескольким счётам и/или валютам. Для накоплений целесообразней открыть сберегательный счёт, который позволит получать фиксированный процент на остаток. Существуют вклады с возможностью досрочного снятия средств. В таком случае денежные средства студента будут застрахованы согласно закону о страховании вкладов (до 1,4 млн. руб.).[9] При этом следует помнить о том, что с 1 января 2021 года доходы по вкладам (остаткам на счетах) будут облагаться налогом на доходы физических лиц[10]. Антон нес потери и при конвертации валюты. Возможно ему следует открыть дополнительную карту в нужной валюте. Другим вариантом прироста накоплений могло бы стать инвестирование на рынке ценных бумаг через приложение банка или открытие металлического счета. Однако стоит учитывать следующую закономерность: чем выше ожидаемая доходность, тем выше риск потери. При выборе объектов и инструментов обязательно помнить о том, что все финансовые риски ложатся на инвестора. Не стоит забывать про комиссии и налоги.

---

[9] Федеральный закон «О страховании вкладов в банках Российской Федерации» от 23.12.2003 № 177-ФЗ http://www.consultant.ru/document

[10] ФНС России разъяснила особенности порядка обложения НДФЛ процентов, полученных по вкладам в банках https://www.nalog.gov.ru/rn77/news/activities_fts/10237437/

Возвращаясь к покупке билетов, следует отметить, что ИИ и технологии банка (фрод-мониторинг) ожидаемо среагировали на данную покупку, распознав её как сомнительную и «нетипичную» операцию для клиента. Транзакция Антона была приостановлена, а карта заблокирована в его интересах, так как зарубежных платежей Антон никогда не проводил, платеж осуществлялся в иностранной валюте. Студент не знал о правилах расчетов и о том, что такая ситуация возможна. Согласно ФЗ «О национальной платежной системе»[11] ст.27 кредитная организация имеет право приостанавливать на срок до 2 рабочих дней исполнение распоряжения клиента о переводе денежных средств при выявлении определённых признаков подозрительной операции. С 01.10.2021 года перечень сомнительных операций расширен на основании Указания ЦБ от 20.10.2020 г. №5599-У. По-видимому, у Антона в контактах телефона не был указан номер обслуживающего банка, и он не отвечал на их звонки. Дело в том, что если банку не удается дозвониться до клиента, то карта блокируется.

Однако из кейса не до конца понятно, почему при обращении Антона в банк процесс разблокировки занял несколько дней. Обычно это происходит сразу после удостоверения личности клиента (кодового слова) и подтверждения необходимости операции при звонке в банк. Это можно сделать и через мобильное приложение банка. Возможно, при обращении в банк Антон не смог оперативно предоставить информацию о себе, чтобы провести процедуру аутентификации и идентификации. Если эти условия были соблюдены, то можно сказать о недоработке банка и его фронт-офиса с запросом клиента (человеческий фактор, проблемы программного обеспечения). Если бы Антон хранил денежные средства раздельно, он смог бы приобрести билеты по другой карте. Еще как вариант, Антон мог обратиться в банк с паспортом, снять деньги с заблокированной карты и провести покупку через карту своих знакомых. Можно посоветовать Антону завести отдельную банковскую карту для интернет-покупок и держать на ней необходимый лимит.

Неудивительно, что, завладев данными карты, мошенники совершили кражу денег без контакта с Антоном. Ему не удалось оспорить транзакцию. Расследование банка и платежной системы однозначно показало, что карта была скомпрометирована. Ее данные попали в руки третьих лиц, которые при совершении платежа (покупки) часов ввели все данные владельца, и платеж не вызвал подозрения у искусственного интеллекта. Если бы клиент не скомпрометировал данные карты и своевременно обратился бы в банк, то средства были бы возвращены. В РФ это регулирует ФЗ «О национальной платежной

[11,14] Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе» http://www.consultant.ru/document

системе»[12], а при международных расчётах действуют правила платежных систем. Средства возвращаются при выполнении двух условий: сообщение данной операции в установленный срок и соблюдение правил безопасности при использовании карты. Возврат гарантирует процедура чарджбэка (chargeback). Так как Антон совершал международные расчеты, значит он пользовался услугами Visa или MasterCard, так как карта Мир имеет ограничения на такие операции. Здесь действуют правила о международных расчетах и существует программа «нулевой ответственности» (см. Приложение 4). В любом случае кража денег – это уголовное преступление и потерпевший должен обратиться не только в банк, но и в полицию.

В кейсе видно, что Антон узнал о проведенной операции только из уведомления банка в личном кабинете. Банк свои обязательства пред клиентом выполнил. Однако из задания не ясно, было ли подключено у Антона смс-оповещение. Получив сообщение, он должен был через личный кабинет проверить списание, обратиться в обсуживающий банк или самостоятельно заблокировать карту. Скомпрометированную карту необходимо перевыпустить. Следовательно, в потери денег виноват сам Антон, а не искусственный интеллект, действовавший исключительно в интересах клиента.

Сгладить ситуацию могло бы наличие у Антона страхового полиса на банковскую карту. Это обеспечило бы ему получение возмещения. Нужно иметь в виду, что это связано с дополнительными расходами для держателя карты.

Заключение (ответы на вопросы задания)

Вопрос 1 (ответить с «позиции бизнеса»): Проанализируйте с позиции кредитной организации, нужны ли какие-то меры по регулированию использования искусственного интеллекта на рынке платежных услуг, и если да, то какие. Ответ обоснуйте.

Цифровизация банковских процессов и использование достижений ИИ позволяет финансовой организации работать более эффективно, обеспечивая интересы бизнеса и своих клиентов. В приложении 5 представлен обзор нормативных документов, регулирующих вопросы ИИ и платежных расчетов как в РФ, так в мире. Анализ показал, что в РФ предприняты значительные шаги по закреплению использования новой технологии и адаптации к международным нормам. Наиболее полной является «Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.»[13] Она поднимает важные для банковского сектора

[13] Распоряжение Правительства РФ от 19.08.2020 №2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» http://www.consultant.ru/document/cons_doc_LAW_360681/f62ee45faefd8e2a11d6d88941ac66824f848bc2/

вопросы использования технологий искусственного интеллекта и персональных данных. Для кредитных организаций кроме норм федерального законодательства важными являются директивы Центрального Банка. Однако ни в одном документе Банка России не дано определение ИИ и правила его использования в кредитных и финансовых организациях. Ключевые вопросы развития финтеха представлены в «Основных направлениях развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов».[14] В них отмечена важность совершенствования процедур идентификации с использованием биометрических технологий и условий оборота обезличенных персональных данных. Таким образом, со стороны регулятора должны быть разработаны правила регулирования и требования обеспечения безопасности данных клиентов, а также стандарты к использованию банковских услуг на основе цифровых технологий и искусственного интеллекта. Именно этих нормативных документов ждут кредитные организации, чтобы на их базе разработать и усовершенствовать свои внутренние документы. Этого будет достаточно для развития ИИ в банковской сфере, поскольку зарегулированность сверху будет тормозит процесс внедрения технологий на местах. Кредитные организации обладают разными финансовыми возможностями, стратегическими целями и уже используемыми возможностями в области ИИ. Тем более банки понимают преимущества ИИ и его роль в защите данных клиентов.

Вопрос 2: Какие возможности и риски, на ваш взгляд, влечет за собой распространение использования искусственного интеллекта на рынке банковских платёжных услуг для личных финансов?

Основная цель внедрения ИИ - повышение эффективности деятельности, масштабирование, автоматизация и качественное управление рисками. Как известно, одним из лидеров по внедрению и использованию высоких технологий является банковский сектор (см. Приложение 6). Введение ИИ предоставляет физическим лицам различные возможности. Во-первых, получение более быстрых ответов на запросы клиентов (чат-боты, голосовые помощники). Во-вторых, повышается скорость непредвзятых скоринговых моделей, а время на одобрение кредитных заявок снижается. В-третьих, увеличивается защита личных финансов при проведении расчетов (ИИ реализует финансовый мониторинг). В-четвертых, клиенты получают доступ к новым цифровым продуктам банков и персонифицированные предложения. SWOT-анализ представлен в приложении 7.

[14] «Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов» (разработаны Банком России) http://www.consultant.ru/document/cons_doc_LAW_404693/

В записке под личным финансовым риском понимается риск, связанный с возможностью потери собственных денежных средств, имущества или другого источника дохода. Авторами были идентифицированы следующие риски на рынке банковских услуг для личных финансов, связанные с использованием кредитными организациями ИИ (см. таблицу 1).

Таблица 1 - Классификация рисков пользователей банковских услуг

Риск	Описание риска
Моральный	заключается в наличие возможности совершения кредитной организацией действий по максимизации собственной выгоды в ущерб клиента
Этический	связан с нарушением прав человека через сбор персональной информации и биометрических данных. Риск может приводить к индивидуальной или групповой дискриминации, цифровому неравенству при доступе к услугам банка
Кибербезопасности (защита персональных данных)	данные клиента могут быть похищены и использованы против него. Сейчас нет возможности для защиты при передаче цифровой подписи клиента
Технический	некачественные данные и некорректная интерпретация результатов могут повлиять на финансы клиента и возможность получения банковской услуги и, как следствие, может возникать риск упущенной выгоды
Ценовой	внедрение ИИ требует значительных инвестиций со стороны кредитной организации, следовательно, возможен рост стоимости предоставляемых услуг
Геополитический	связаны с политической обстановкой. Клиенты банков, попавших под санкции, лишаются возможности получения ряда услуг, в т.ч. платежных (Mastercard и Visa), использования приложения банка из App Store и Google play (невозможность получения онлайн обслуживания)
Отсутствия прозрачности данных	пользователи банков, использующих ИИ, не осведомлены о методах сбора, передачи и хранения персональных данных

Подводя итоги, можно сделать следующие выводы:

1. Мегарегуляторы развитых и развивающихся стран активно поддерживают и регулируют использование цифровых технологий в финансовой сфере.

2. Кредитные организации и платёжные системы заинтересованы в ИИ и осуществляют инвестиции в данные технологии. Цифровизация направлена не только на сокращение операционных расходов и повышение доходов, но и на автоматизацию внутренних процессов, идентификацию и аутентификацию, обнаружение мошеннических операций.

3. ИИ должен работать в интересах бизнеса и минимизировать риски клиентов. Однако, не всегда удается избегать ситуаций, когда операции происходят без согласия клиентов.

4. Клиенты кредитных организаций также должны думать о безопасности своих сбережений, действовать рационально, уделять дополнительное внимание изучению вопросов финансовой безопасности и использовать превентивные действия, направленные на минимизацию рисков.

5. Повышается роль этики больших данных. Так, в 2019 году Институтом развития интернета (ИРИ) и Ассоциацией участников рынка больших данных был разработан Кодекс этики использования данных. По информации на 2020 год к данному документу присоединились 24 российские компании, в том числе и кредитные организации.

Цифровые технологии переживают период расцвета, что сопряжено с возможными временными недоработками. ИИ направлен на защиту интересов клиента, но переоценивать уровень развития современных технологий не стоит. Ситуация кейса еще раз поднимает вопрос личной ответственности человека за обеспечение финансовой и информационной безопасности. Ведь если бы Антон более внимательно относился к управлению своими финансами, то не произошло бы и потери денежных средств.

Список использованных источников

1. О национальной платежной системе: ФЗ от 27.06.2011 161-ФЗ (ред. от 02.07.2021) [Электронный ресурс] СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/b0062cfb1c3cae710d57f0557303e78760a31d16/ (Дата обращения: 15.01.2022).

2. О страховании вкладов в банках Российской Федерации: ФЗ от 23.12.2003 №177 [Электронный ресурс] СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/document (Дата обращения: 20.02.2022).

3. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: ФЗ от 31.07.2020 №258 [Электронный ресурс] СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru (Дата обращения: 20.01.2022).

4. О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21 июля 2020 г. № 474 [Электронный ресурс] СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_357927/ (Дата обращения: 17.01.2022).

5. Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года: Распоряжение Правительства РФ от 19.08.2020 №2129-р [Электронный ресурс] СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_360681/f62ee45faefd8e2a11d6d88941ac66824f848bc2/ (Дата обращения: 20.01.2022).

6. Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов: разработаны Банком России [Электронный ресурс] СПС КонсультантПлюс - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_404693/ (Дата обращения: 19.01.2022).

7. Ассоциация ФинТех - Официальный Интернет-сайт [Электронный ресурс]. – Режим доступа: https://www.fintechru.org (дата обращения: 25.02.2022).Как применяется искусственный интеллект на финансовых рынках [Электронный ресурс]. - Официальный Интернет-сайт РБК+ Режим доступа: https:// plus.rbc.ru/partners/61c970c07a8aa98f36771580 (Дата обращения: 20.01.2022).

8. Исследование: крупные банки чаще используют искусственный интеллект [Электронный ресурс]. – Официальный Интернет-сайт РБК+ Режим доступа: Frank.RG: https://frankrg.com/12651 (Дата обращения: 29.01.2022).

9. Как устроен антифрод и почему с мошенниками так сложно бороться [Электронный ресурс]. – Официальный Интернет-сайт РБК+ Режим доступа:

https://trends.rbc.ru/trends/industry/6167ff259a7947f4c6908e46 (Дата обращения: 27.01.2022).

10. Статистика национальной платежной системы - Официальный Интернет-сайт [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/nps/psrf/ (Дата обращения: 25.02.2022).

11. Учебное пособие по финансовой грамотности [Электронный ресурс]. – Режим доступа: https://finuch.ru/ (Дата обращения: 01.02.2022).

12. ФНС России разъяснила особенности порядка обложения НДФЛ процентов, полученных по вкладам в банках - Официальный Интернет-сайт Федеральной налоговой службы [Электронный ресурс]. – Режим доступа: https://www.nalog.gov.ru/rn77/news/activities_fts/10237437/ (Дата обращения: 15.02.2022).

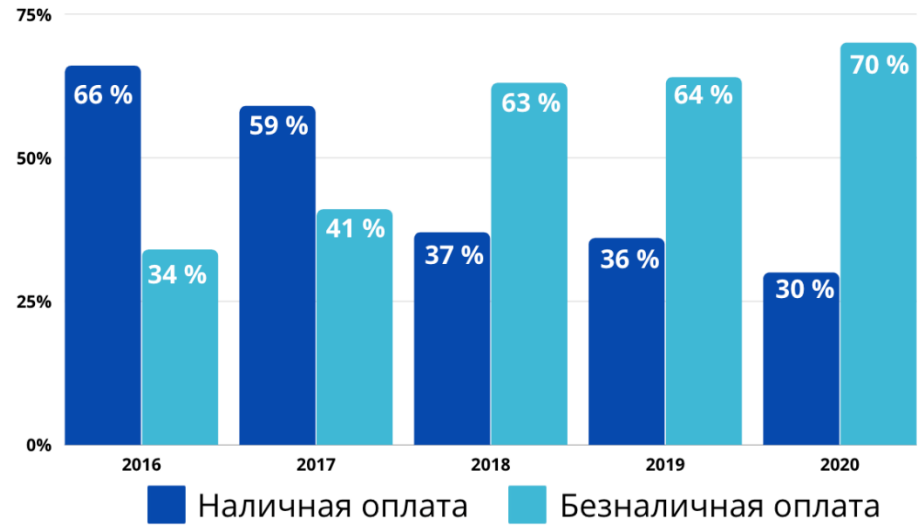
13. Цифровая трансформация отраслей: стартовые условия и приоритеты: докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2021. — 239, [1] с. — ISBN 978-5-7598-2510-4 (в обл.). — ISBN 978-5-7598-2270-7 (e-book) https://conf.hse.ru/mirror/pubs/share/463148459.pdf. (Дата обращения 22.02.2022).

14. OECD (2019). Science and Technology vectors of Digital Transformation - Официальный Интернет-сайт [Электронный ресурс]. – Режим доступа: - https://www.oecd-ilibrary.org (Дата обращения 12.02.2022).

15. Visa - Официальный Интернет-сайт [Электронный ресурс]. – Режим доступа: - https://usa.visa.com/run-your-business/visa-security/risk-solutions/authorization-optimization.htm (Дата обращения 10.02.2022).

Приложение 1

Предпочтения населения РФ относительно формы оплаты

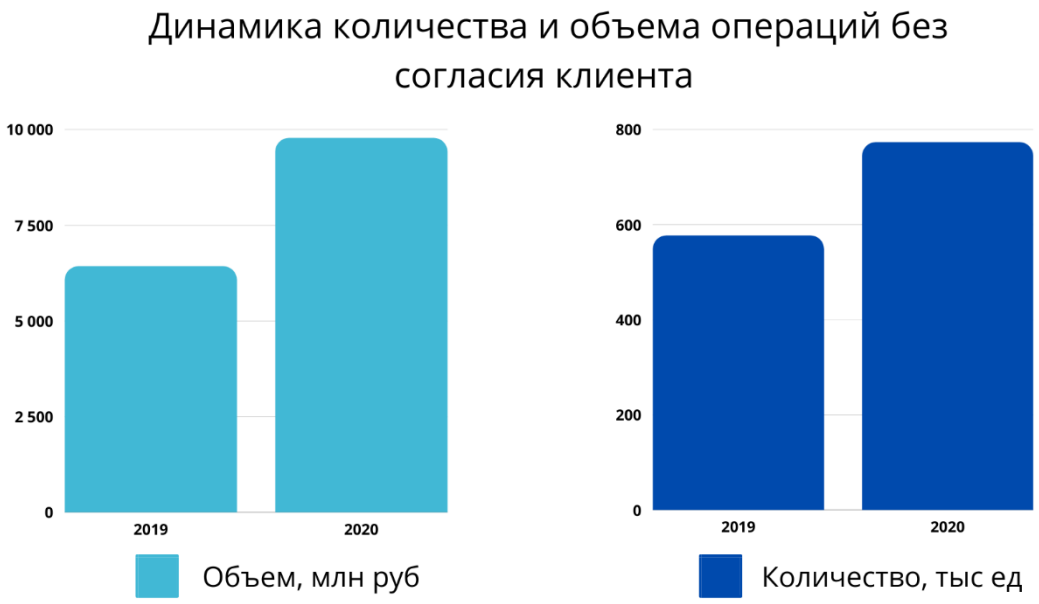


Источник: составлено авторами на основании открытых данных ЦБ РФ https://cbr.ru/

Приложение 2

Источник: составлено авторами на основании открытых данных ЦБ РФ https://cbr.ru/

Приложение 3



Источник: составлено авторами на основании открытых данных ЦБ РФ https://cbr.ru/

Мошеннические интернет-ресурсы — выявлено (ед.), заблокировано (%)

	2019	2020
	III квартал	III квартал
Фишинг	0	70 ▸84%
ВПО	160 ▸99%	8 ▸100%
Лжебанк	132 ▸86%	375 ▸95%
МФО	44 ▸43%	31 ▸65%
Профессиональный участник РЦБ	141 ▸16%	125 ▸37%
Остальные виды мошенничества	2 325 ▸48%	1 540 ▸92%

Источник: ЦБ РФ https://cbr.ru/

Приложение 4

СРАВНЕНИЕ VISA И MASTERCARD

Visa первой начала использовать нейронные сети, воспроизводящие структуру человеческого мозга, в качестве основы ее платформы ИИ для выявления возможных мошеннических операций. Компания работает с системой Visa Advanced Authorization (VAA), работающая на базе искусственного интеллекта, которая, анализируя большие объемы данных по транзакциям, умеет более точно выявлять мошеннические действия.

VAA оценивает 100% авторизаций по картам Visa (более 65 тысяч в секунду), которые проходят через сеть платежной системы. Благодаря этой системе Visa предотвращает мошеннические операции на сумму около 25 млрд долл ежегодно.

В случае необходимости оспаривания какой-либо транзакции Visa рекомендует пользователям обратиться к эмитенту карты или в банк по бесплатному номеру, указанному на лицевой или оборотной стороне карты Visa. Если клиент Visa столкнулся с кражей идентификационных данных, то ему необходимо посетить веб-сайт https://callforaction.org/ и обратиться на страницу «Утеря или кража карты» на официальном сайте платежной системы.

Политика нулевой ответственности Visa — гарантия отсутствия у покупателя ответственности за несанкционированное списание со счета или с использованием информации о счете. Клиент защищен на случай утери или кражи кредитной или дебетовой карты Visa или ее мошеннического использования онлайн или в торговых точках. Держатель карты должен позаботиться о защите своей карты и немедленно уведомить финансовое учреждение, выдавшее карту, о ее несанкционированном использовании.

СРОК РАССМОТРЕНИЯ ЗАЯВЛЕНИЙ НА CHARGEBACK.

120 ДНЕЙ

Мировая платежная система MasterCard использует комплексный сервис Decision Intelligence для принятия решений и выявления мошенничества. Сервис использует технологию искусственного интеллекта для того, чтобы помочь финансовым институтам повысить точность разрешений для немошеннических транзакций в режиме реального времени и уменьшить число ложных отказов.

Только в США сумма ошибочных отказов превышает сумму потерь от настоящего мошенничества с платежными картами в 13 раз.

Mastercard ChargeBack guide содержит условия, при которых эмитент может обрабатывать первый возвратный платеж вследствие мошенничества в соответствии с возвратным платежом без авторизации держателя карты:

- Владелец карты связался с эмитентом, утверждая, что владелец карты не санкционировал транзакцию.
- О транзакции было сообщено в базу данных о мошенничестве и убытках как о мошенничестве в соответствии с Руководством пользователя базы данных о мошенничестве и убытках не позднее даты отзыва платежа.
- Держатель карты предоставил электронную почту держателя карты, письмо, сообщение или заполненную форму разрешения споров о мошенничестве (форма 0412), в которой указывается, что держатель карты не санкционировал транзакцию.

СРОК РАССМОТРЕНИЯ ЗАЯВЛЕНИЙ НА CHARGEBACK.

120 ДНЕЙ

Источник: составлено авторами на основании открытых данных с https://www.visa.com.ru/ и https://www.mastercard.ru/

Приложение 5

СРАВНЕНИЕ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ

Нормативно-правовое регулирование расчетов в РФ

- Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ. Глава 46
- Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ
- Положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств» (Зарегистрировано в Минюсте России 25.08.2021 № 64765)
- Указание ЦБ РФ от 20.10.2020 № 5599-У «О внесении изменений в положение Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»

Нормативно-правовое искусственного интеллекта в РФ

- Указ Президента РФ от 10 октября 2019 г. № 490 «О развитие искусственного интеллекта в Российской Федерации»
- Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31.07.2020 № 258-ФЗ.
- Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»
- Распоряжение Правительства РФ от 19.08.2020 г. №2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.».

Нормативно-правовое искусственного интеллекта и расчетов в мире

- Проект Регламент Европейского союза «О европейском подходе для искусственного интеллекта» (Regulation on a European Approach for Artificial Intelligent) и совместного заключения на данный проект EDPB и EDPS от 18.06.2021 г.
- Правила платежной системы Виза по осуществлению операций на территории Российской Федерации Visa Payment System Operating Regulations - Russia (30 декабря 2018)
- The Rules of the Mastercard Payment System in Russia Edition 7 Правила платёжной системы «Мастеркард» в России Редакция №7 17 June 2020

Источник: составлено авторами

Приложение 6

Победители рейтинга SDI360° Топ-10 компаний

Место	Общее кол-во баллов	Название компании	Место по активам	Активы на 01.04.2021, млрд. руб.	Рейтинг по категориям, **место** / количество баллов		
					Представ-ленность в интернете	Продвиже-ние и ком-муникации	Онлайн-продажи
1	260	**Альфа-Банк**	5	4 609	**1** 95	**1** 80	**3** 85
2	255	**Райффайзенбанк**	10	1 406	**2** 90	**2** 80	**4** 85
3	255	**Тинькофф Банк**	15	795	**3** 90	**5** 70	**1** 95
4	230	**Сбербанк**	1	32 711	**13** 70	**3** 80	**5** 80
5	220	**Открытие**	8	2 473	**7** 75	**6** 70	**9** 75
6	210	**Россельхозбанк**	6	3 674	**8** 75	**4** 75	**30** 60
7	195	**Газпромбанк**	3	7 107	**5** 80	**20** 40	**10** 75
8	190	**ВТБ**	2	16 204	**9** 75	**7** 65	**39** 50
9	190	**Росбанк**	11	1 319	**16** 65	**10** 50	**11** 75
10	185	**Совкомбанк**	9	1 551	**4** 85	**33** 30	**15** 70

Источник: Исследование цифровой зрелости банков агенства цифрового аудита SDI360 https://sdi360.ru/banks

Приложение 7

SWOT-анализ влияния искусственного интеллекта на личные финансы граждан РФ

*Источник: составлено авторами