Евразийская адвокатура. 2022. № 2 (57). С. 90.
Eurasian advocacy. 2022;(2(57)):90.

Правосудие и правоохранительная деятельность в евразийском пространстве

Научная статья
УДК 343.9
doi 10.52068/2304-9839_2022_57_2_90

# ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ В БАНКОВСКОЙ СФЕРЕ

**Багреева Елена Геннадиевна[1], Исмаилов Нурлан Элман оглы[2], Бобылева Лилия Михайловна[3]**
[1]Доктор юридических наук, профессор, профессор Департамента международного и публичного права Финансового университета при Правительстве Российской Федерации
125167, г. Москва, Ленинградский пр-т , д. 49/2, Российская Федерация
[2]Студент Финансового университета при Правительстве Российской Федерации
125167, г. Москва, Ленинградский пр-т , д. 49/2, Российская Федерация
[3]Студент Финансового университета при Правительстве Российской Федерации
125167, г. Москва, Ленинградский пр-т , д. 49/2, Российская Федерация

**Аннотация:** Авторы научной работы рассматривают проблему мошенничества в банковской сфере и приходят к выводу о необходимости внедрения нового механизма в борьбе с такого рода преступлениями – искусственного интеллекта (ИИ). Изучив риски использования ИИ, авторы утверждают, что данный инструмент намного повысит эффективность противодействия мошенничеству при наличии действующих мер по борьбе с киберпреступностью.

**Ключевые слова:** мошенничество, противодействие мошенничеству, несанкционированные транзакции, кража данных карты, искусственный интеллект, анализ транзакций

**Для цитирования:** Багреева Е.Г., Исмаилов Н.Э., Бобылева Л.М. Искусственный интеллект как противодействие мошенничеству в банковской сфере // Евразийская адвокатура. 2022. № 2 (57). С. 90. https://doi.org/10.52068/2304-9839_2022_57_2_90

Justice and law-enforcement activity In the eurasian space

Original article

# ARTIFICIAL INTELLIGENCE AS A COUNTERACTION TO FRAUD IN THE BANKING SECTOR

**Bagreeva Elena Gennadievna[1], Ismailov Nurlan Elman ogly[2], Bobyleva Lilia Mikhailovna[3]**
[1]LLD, Professor, Professor of the Department of International and Public Law of the Financial University under the Government of the Russian Federation
125167, Moscow, Leningradsky Ave., 49/2, Russian Federation
[2]Student of the Financial University under the Government of the Russian Federation
125167, Moscow, Leningradsky Ave., 49/2, Russian Federation
[3]Student of the Financial University under the Government of the Russian Federation
125167, Moscow, Leningradsky Ave., 49/2, Russian Federation

**Abstract:** The authors of the research consider the problem of fraud in the banking sector and conclude about the necessity to introduce a new mechanism in the fight against this kind of crime – artificial intelligence. After examining the risks of using AI, the authors argue that this tool would greatly increase the effectiveness of counter-fraud with existing anti-crime measures.

**Keywords:** fraud, anti-fraud, unauthorized transactions, card identity theft, artificial intelligence, transaction analysis

**For citation:** Bagreeva E.G., Ismailov N.E., Bobyleva L.M. Artificial intelligence as a counteraction to fraud in the banking sector= Eurasian advocacy. 2022;2(57): 90. (In Russ.). https://doi.org/10.52068/2304-9839_2022_57_2_90

Банковская сфера всегда являлась одним из самых притягательных мест для криминальных посягательств: получение денежной выгоды делает банковские учреждения более уязвимыми для мошенничества, поскольку именно в них хранится большая часть денег. Сегодня в условиях нарастания темпов мошенничества в банковской сфере необходимо противопоставить преступлениям новые инструменты борьбы.

© Багреева Е.Г., Исмаилов Н.Э., Бобылева Л.М., 2022

21 марта 2022 года компанией Sift (разработчик инструментов для реагирования на киберпреступления) был выпущен отчет за 2021 год, который описывает все более сложные и часто автоматизированные тактики, используемые киберпреступниками для совершения мошенничества с платежными системами. Рассчитанный на основе данных глобальной сети, включающей более 34 тысяч сайтов и приложений, индекс показывает, что в 2021 году уровень мошеннических действий с платежами резко вырос – на 70 %, что является самым высоким показателем среди всех секторов сети [1].

В этой связи целесообразно обратить внимание на использование искусственного интеллекта (ИИ), ставшегося еще в 2018 году на основе Указа Президента «О национальных целях и стратегических задачах развития РФ на период до 2024 года» значимым элементом цифровизации экономики [2].

Сокращение масштабов мошенничества является первостепенной задачей для банков, поскольку напрямую влияет на итоговый результат их работы. Однако мошенничество не только наносит финансовый ущерб банкам, но и представляет собой угрозу статусу организации и ее взаимодействию с внешними заинтересованными сторонами, такими как клиенты, поставщики, финансисты и деловые партнеры. Действительно, мошеннические действия наносят ущерб их репутации, приводят к отрицательному пользовательскому опыту и снижают уровень доверия клиентов. Таким образом, банки постоянно вынуждены развивать систему борьбы с преступлениями и изучать новые возможности в данной сфере.

Виды мошенничества, выявляемые в сфере банковских услуг, разнообразны. Рассмотрим несколько наиболее распространенных видов банковского мошенничества:

– несанкционированные транзакции, т. е. банковские операции, или операции с кредитными картами, которые владелец счета не совершал или не одобрял, по-прежнему доставляют неудобства как банкам, так и потребителям [3]. В статье Forbes сообщается, что примерно восемь из десяти пользователей мобильных банковских услуг обеспокоены мошенничеством с кредитными картами. Кроме того, по прогнозам Statistica, стоимость мошеннических операций с платежными картами в мире к 2027 году может вырасти до 38,5 миллиардов долларов;

– скимминг – незаконный процесс дублирования информации, содержащейся на магнитной полосе кредитной карты [4]. Обычно это происходит при потере или краже кредитной или дебетовой карты, так как мошенник может снять данные с магнитной полосы или использовать карту в Интернете, применив ее данные. Хотя мошенники не могут снять наличные без ПИН-кода карты, они могут использовать карту для бесконтактной оплаты, если эта функция включена на карте. Кроме того, известно, что некоторые ритейлеры и торговцы злоупотребляют банковской информацией клиентов, похищая копии учетных данных при использовании карты во время покупки;

– личное мошенничество, часто совершаемое путем подглядывания через плечо человека с использованием банкомата или тактики отвлечения внимания. Это опасный вид финансового мошенничества, поскольку мошенник может получить доступ к банковской карте и ПИН-коду своей жертвы. Иногда преступник может вовлечь жертву в разговор, чтобы узнать о ней больше идентифицирующей информации. Как и скимминг, карта может быть использована различными способами, но с добавлением ПИН-кода и любой другой информации открываются новые возможности, включая покупки в розничной торговле лицом к лицу [5];

– телефонное банковское мошенничество заключается в том, что преступник пытается убедить клиента добровольно передать информацию или перевести свои деньги на другой счет. Мошенник обычно пытается убедить клиента, что ему необходимо перевести деньги, чтобы не потерять их и защитить свои активы. Он может даже выдумывать фальшивые правонарушения и требовать, чтобы объект заплатил штраф за их совершение;

– мошенничество со счетами-фактурами. Этот пример банковского мошенничества направлен на предприятия, когда мошенники, обычно по электронной почте, выдают себя за поставщика, доказывая необходимость обновить банковские реквизиты, по которым оплачиваются счета. Это может выглядеть совершенно невинно, если мошенник взломал данные поставщика, так как запрос будет выглядеть подлинным. Яркий пример мошенничества такого рода имел место в 2013–2015 годах, когда Facebook и Google стали жертвами преступления, которое обошлось им более чем в 100 миллионов долларов. В этом конкретном случае мошенничества в сфере онлайн-банкинга литовский хакер выдавал себя за азиатского производителя и отправлял поддельные счета-фактуры технологическим гигантам [5];

– мошенничество в сфере онлайн-банкинга может иметь множество обличий, включая фи-

шинг, атаки вредоносных программ, мошенничество с использованием «сомов» и сайтов-клонов. Поскольку так много банковских операций осуществляется через интернет, неудивительно, что это распространенный вид банковского мошенничества.

Мошенники становятся все более искусными в создании убедительных электронных писем и веб-сайтов, что затрудняет защиту жертв. Примером банковского мошенничества в интернете может быть звонок мошенника, который выдает себя за сотрудника банка, сообщая жертве, что ее счет был взломан и ей необходимо перевести деньги на другой счет. Или же мошенник просит жертву подтвердить ПИН-код, пароль счета или уточнить данные по электронной почте, опять же выдавая себя за законных сотрудников банка;

– кража идентификационных данных карты. Этот вид банковского мошенничества может включать в себя завладение законным банковским счетом и выдачу себя за его владельца или использование украденных или поддельных документов для открытия счета на чужое имя [6]. Кража личных данных является наиболее распространенным видом жалоб, подаваемых потребителями, и оказывает серьезное влияние как на потребителей, так и на финансовые учреждения. Только в 2020 году общие финансовые потери от мошенничества с идентификационными данными составили, согласно результатам исследования Javelin 2021 Identity Fraud Survey, около 13 миллиардов долларов США.

Как видим, существует огромное количество видов мошенничества в банковской сфере, и данный перечень далеко не исчерпывавший. Ущерб от преступлений как для компаний, так и для обычных пользователей банковскими услугами колоссальный, в связи с чем необходимо развивать систему мер борьбы с преступностью.

В современной России основным способом борьбы с мошенничеством является информирование населения о преступных схемах мошенников. Выражается это в предупреждении населения о соблюдении следующих мер безопасности.

Во-первых, необходимо держать в тайне следующие данные: коды из SMS и PUSH-уведомлений, ПИН-код карты, контрольные вопросы, данные карты, включая срок действия и трехзначный код. Нельзя также раскрывать персональные данные: отчество, место и год рождения, данные паспорта [7].

Во-вторых, в связи с участившимися случаями телефонного мошенничества не следует доверять незнакомым абонентам, даже если они представляются сотрудниками банка. В таких случаях необходимо позвонить на официальный номер своего банка и убедиться, звонили ли его сотрудники на самом деле.

В-третьих, при потере карты необходимо сразу связаться с банком, чтобы заблокировать ее для сохранения сбережений, а затем выпустить новую карту, на которую и будут переведены накопленные сбережения.

Тем не менее, данные меры не могут в полной мере защитить пользователей от мошенников. Существует человеческий фактор. Людям свойственно доверять, паниковать, быть невнимательными, поэтому невозможно обеспечивать защиту от мошенничества простым информированием населения. Данный метод должен быть дополнительным, и полагаться на него крупным банковским организациям не стоит.

Одним из наиболее действенных методов является проверка операций банком плательщика, когда производятся подозрительные действия, например, единоразово переводится большая сумма денег. Как показывают практика и жизненный опыт, к сожалению, не всегда удается предотвратить мошенничество с помощью проверки. Данный метод, как правило, работает при переводе крупной суммы денег. Недавно Центральный Банк РФ объявил, что такую же проверку финансовых операций будут проводить и банки получателя платежа, что, конечно же, увеличит эффективность борьбы с преступностью.

«Доступ к счету получателя будет ограничиваться с соблюдением гражданских прав его владельца, – подчеркнули в Банке России. – Это означает, что он сможет распорядиться деньгами, но для этого нужно будет прийти в офис банка с паспортом» [8].

Таким образом, на сегодняшний день система мер по борьбе с мошенничеством в банковской сфере основана на действиях двух субъектов: пользователя и банка. Банк надеется, что пользователь будет внимательным при совершаемых им операциях, не будет переходить по незнакомым ссылкам на незнакомые сайты и доверять абонентам, представляющимся сотрудниками банка. С другой стороны, пользователь надеется, что банк сможет защитить и обезопасить его от мошенников, даже если деньги оказались в руках преступника.

В современной России данные меры, конечно же, работают, однако уровень преступности повышается в силу того, что сами мошенники находят все более и более уязвимые места. Именно поэтому в конце 2021 года Центральный Банк РФ

разработал план поправок к Федеральному закону 61-ФЗ «О национальной платежной системе», который должен будет обезопасить жертв мошенничества. Следовательно, вопрос о необходимости улучшения системы мер безопасности банковских операций актуален [9].

В распоряжении банков уже есть секретное оружие, которое можно использовать для выявления и предотвращения мошенничества, – искусственный интеллект. Он уже используется банками для предоставления услуг клиентам и совершенствования бизнес-процессов. Но расцвет этой технологии еще впереди. Банки приходят к выводу, что использование ИИ является наиболее быстрым и эффективным способом выявления мошенничества.

В 2021 году издание Fintech News сообщило, что финансовые учреждения внедряют системы на основе ИИ в рекордном количестве, при этом более 217 миллиардов долларов США было потрачено на приложения ИИ для предотвращения мошенничества и оценки рисков [10]. Еще более многообещающим является тот факт, что 64 % финансовых учреждений считают, что ИИ может опередить мошенничество до того, как оно произойдет.

В отечественной практике внедрение ИИ не связано с противодействием преступности, однако мы рассмотрим ряд обстоятельств, в которых ИИ мог бы наиболее эффективно использоваться не только для упрощения предоставления услуг, но и с точки зрения безопасности.

Существует ряд способов применения ИИ для выявления мошенничества в сфере финансовых услуг. Одной из основных функций его является анализ транзакций. Каждое приложение – от оценки рисков до группировки потребителей в идентифицируемые кластеры или «профили» – имеет важное значение для построения надежной стратегии обнаружения мошенничества различными способами:

1. Построение профилей покупок.

Для точного выявления мошенничества финансовые учреждения должны сначала понять, как выглядит типичное поведение клиентов. Используя машинное обучение для сортировки огромного количества данных о прошлых финансовых и нефинансовых операциях, банки могут создавать и распределять клиентов по нескольким различным профилям. Профили полезны тем, что дают актуальную картину активности по счету и помогают делать прогнозы относительно будущего поведения. Например, счет клиента может быть профилирован как «питающийся в ресторанах по выходным», «совершающий регулярные ежеквартальные поездки в Санкт-Петербург» или «заправляющий свой автомобиль бензином после работы». Один и тот же счет может быть помещен в сотни различных профилей на основе его активности, причем профиль обновляется в режиме реального времени после каждой транзакции. По мере совершения транзакций искусственный интеллект определяет, соответствуют ли они шаблону или же их можно пометить как достаточно сильно отличающиеся от нормы.

2. Разработка оценок мошенничества.

Всем транзакциям может быть присвоен балл мошенничества на основе данных о прошлых законных транзакциях, случаях мошенничества и параметрах риска, установленных финансовым учреждением. Этот показатель, учитывающий такие переменные, как сумма транзакции, время, частота использования карты, IP-адрес покупки и многое другое, используется для оценки риска мошенничества, связанного с данной конкретной транзакцией. Оценка риска мошенничества используется для автоматического одобрения транзакции, пометки ее на пересмотр или полного отказа от нее. С помощью машинного обучения точность оценок мошенничества со временем повышается.

3. Расследование мошенничества.

Алгоритмы машинного обучения могут анализировать сотни тысяч транзакций в секунду. Нейронные сети расширяют эти возможности, принимая решения в режиме реального времени. Эти технологии успешно справляются с неуправляемым количеством отмеченных транзакций и предоставляют краткий список тех, которые требуют дальнейшего расследования со стороны человека. Расследование и судебное преследование заявлений о мошенничестве может отнимать невероятно много времени, поэтому важно, чтобы агенты были вооружены надлежащими инструментами для повышения эффективности. Применение дополненного интеллекта может помочь командам определить приоритеты и оптимизировать расследования.

4. Знай своего клиента.

Искусственный интеллект может практически мгновенно проверять удостоверения личности и документы, сопоставлять отпечатки пальцев и даже выполнять распознавание лиц. На основе ИИ можно будет быстро реагировать на мошенничества при использовании карты другим лицом. ИИ будет знать своего клиента, а при отклонениях данных сообщать об этом или же не осуществлять желаемую данным лицом операцию.

Научное сообщество начинает изучать вопросы, связанные с безопасностью, этичностью и экономическими последствиями применения ИИ. Искусственный интеллект должен быть объективен, справедлив в принятии решений, находиться под контролем человеком. В таких ситуациях, когда, например, принимается решение о выдаче кредита, ИИ не должен опираться на характеристики о поле человека, его расовой и национальной принадлежности.

К рискам можно отнести выход систем из-под контроля и причинение вреда человеку и обществу, непонимание и непредсказуемость алгоритмов, недостаточную устойчивость и надежность систем принятия решений. Зачастую сложно выяснить, почему искусственным интеллектом выбрано то или иное решение. Это может вызывать недоверие к системам, использующим технологии ИИ.

Результат работы моделей ИИ зависит от значительного объема данных из различных, в том числе внешних, источников. Это повышает требования к системам информационной безопасности для компенсации рисков намеренного искажения входных данных.

Для устранения этих рисков, например, Сбербанк одним из первых в России утвердил принципы этики ИИ. Они дают сотрудникам ориентиры, как поступать в ситуациях этических дилемм, которые могут возникнуть при взаимодействии с ИИ. ВТБ для решения этих проблем внедрил систему управления моделями [11].

Таким образом, перспективы использования искусственного интеллекта очевидны. Более того, в некоторых сферах существует необходимость в ИИ еще и в силу более быстрой переработки большого количества информации, на что человек объективно не способен. Однако существуют риски, которые следует учитывать при использовании ИИ, чтобы избежать последствий, наносящих ущерб не только финансового, технического, но и репутационного характера.

Искусственный интеллект – новая возможность для банков и пользователей обезопасить свои сбережения, вклады. Конечно, существуют определенные риски, однако без внедрения ИИ рисков по потере денежных средств будет ещё больше. Тем более, что иностранные организации уже используют преимущества ИИ для обеспечения безопасности финансовых операций.

Таким образом, учитывая увеличение количества мошеннических действий в банковской сфере и, соответственно, жертв, согласимся с тем, что действующая система противодействия мошенникам в этой сфере в определенной мере способствуют защите пользователей от нападок, однако, на наш взгляд, еще остаются резервы.

Потребители продолжают надеяться на то, что финансовые учреждения предоставят им возможность осуществлять банковские операции на ходу и получать доступ к своей информации в режиме онлайн. В то же время они ожидают, что их банк создаст среду, в которой эти транзакции будут выполнены безопасным и надежным образом. Целесообразно продолжать оперативно информировать население о новых видах мошенничества и предупреждать о наличии подозрительных операций [12].

Внедрение же искусственного интеллекта обезопасит выполнение большинства денежных операций: можно будет быстрее и эффективнее распознавать новые виды мошенничества и предоставлять необходимую информацию сотрудникам, а также обнаруживать подозрительные операции и предотвращать их проведение. Использование возможностей искусственного интеллекта значительно усилит действующие меры противодействия и создаст синергетический эффект по борьбе с мошенничеством в банковской сфере.

**Список источников**

1. Мошенничество с банковскими картами и платежами [Электронный ресурс]. URL: https://tadviser.ru.
2. Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [Электронный ресурс]. URL: https://mvd.consultant.ru.
3. Смолин С.В. Мошенничество с использованием платежных карт // Законность. 2016. № 1. С. 49–51.
4. Пойманова Л.А. Мошенничество в банковской сфере: понятие, признаки, виды // Сибирский юридический вестник. 2018. № 2. С. 84–89.
5. Журкина О.В. Актуальные проблемы предупреждения мошенничества с использованием платежных карт // Вестник Вятского государственного университета. 2014. № 9. С. 117–121.
6. Fourteen Key Types of Banking Fraud [Электронный ресурс]. URL: https://www.stpaulschambers.com.
7. Абдуллаева Т.Т.К., Бурликова Т.В. Финансовые преступления в России: сущность и особенности // Студенческий вестник. 2020. №19 (117). С. 13–16.
8. Блокировать и замораживать. Как Госдума предлагает бороться с мошенниками [Электронный ресурс]. URL: https://www.gazeta.ru.
9. Седых Ю.Н. Мошенничество в кредитно-банковской сфере // Молодой ученый. 2012. № 3. С. 190–192.
10. How is AI transforming fraud detection in banks? [Электронный ресурс]. URL: https://www.telusinternational.com.
11. Искусственный интеллект в финансах: как банки используют нейросети [Электронный ресурс]. URL: https://trends.rbc.ru.

12. Современная парадигма трансформации миропорядка // Самоуправление. 2021. № 4. С. 221–224.

## References

1. Moshennichestvo s bankovskimi kartami i platezhami [E`lektronny`j resurs]. URL: https://tadviser.ru.
2. Ukaz Prezidenta RF ot 7 maya 2018 g. № 204 «O nacional`ny`x celyax i strategicheskix zadachax razvitiya Rossijskoj Federacii na period do 2024 goda» [E`lektronny`j resurs]. URL: https://mvd.consultant.ru.
3. Smolin S.V. Moshennichestvo s ispol`zovaniem platezhny`x kart // Zakonnost`. 2016. № 1. C. 49–51.
4. Pojmanova L.A. Moshennichestvo v bankovskoj sfere: ponyatie, priznaki, vidy` // Sibirskij yuridicheskij vestnik. 2018. № 2. S. 84–89.
5. Zhurkina O.V. Aktual`ny`e problemy` preduprezhdeniya moshennichestva s ispol`zovaniem platezhny`x kart // Vestnik Vyatskogo gosudarstvennogo universiteta. 2014. № 9. S. 117–121.
6. Fourteen Key Types of Banking Fraud [E`lektronny`j resurs]. URL: https://www.stpaulschambers.com.
7. Abdullaeva T.T.K., Burlikova T.V. Finansovy`e prestupleniya v Rossii: sushhnost` i osobennosti // Studencheskij vestnik. 2020. №19 (117). S. 13–16.
8. Blokirovat` i zamorazhivat`. Kak Gosduma predlagaet borot`sya s moshennikami [E`lektronny`j resurs]. URL: https://www.gazeta.ru.
9. Sedy`x Yu.N. Moshennichestvo v kreditno-bankovskoj sfere // Molodoj ucheny`j. 2012. № 3. S. 190–192.
10. How is AI transforming fraud detection in banks? [E`lektronny`j resurs]. URL: https://www.telusinternational.com.
11. Iskusstvenny`j intellekt v finansax: kak banki ispol`zuyut nejroseti [E`lektronny`j resurs]. URL: https://trends.rbc.ru.
12. Sovremennaya paradigma transformacii miroporyadka // Samoupravlenie. 2021. № 4. S. 221–224.

*Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.*
*Авторы заявляют об отсутствии конфликта интересов.*

*Contribution of the authors: the authors contributed equally to this article.*
*The authors declare no conflicts of interests.*

*Статья поступила в редакцию 02.05.2022; одобрена после рецензирования 10.05.2022; принята к публикации 11.05.2022.*

*The article was submitted 02.05.2022; approved after reviewing 10.05.2022; accepted for publication 11.05.2022.*

