4/2024, iyul-avgust (№ 00072)

ОБ ИСПОЛЬЗОВАНИИ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БАНКОВСКОЙ СФЕРЕ

Очилов Акрам Одилович
Каршинский государственный университет, Узбекистан, DSc., профессор, академик Академии наук Туран
ORCID: *0009-0004-9254-188X*
E-mail: *akram.oo@mail.ru*

Коновалова Ольга Александровна
Санкт-Петербургский политехнический университет Петра Великого, Россия, к.т.н., доцент
ORCID: *0000-0002-3072-3504*
E-mail: *danilenkoolga@mail.ru*

Аборкина Екатерина Оскаровна
PhD, журнал «В центре экономики», Россия, главный редактор
ORCID: 0000-0003-1344-3604
E-mail: melcaseo@mail.ru

Кадиров Лутфулла Халимович
Каршинский государственный университет, докторант
ORCID: 0009-0006-1630-8220
E-mail: L.Qodirov@mail.ru

Акимов Степан Андреевич
Санкт-Петербургский политехнический университет Петра Великого, Россия, магистрант.
ORCID: 0009-0001-7526-5228
E-mail: stepan.akimov02@gmail.com

Тураева Мехринисо Рустамовна
Каршинский государственный университет, магистрант
E-mail: mehrinisoturaeva@gmail.com
DOI: *https://doi.org/10.55439/EIT/vol12_iss4/i12*

Аннотация
Статья посвящена актуальным вопросам снижения числа мошеннических операций в отношении денежных средств клиентов банков. От года к году число таких финансовых преступлений растет, что в свою очередь негативно влияет на имиджевую компоненту банков,

а также приводит к огромным потерям не только со стороны клиентов, но и со стороны банков в части возмещения этого ущерба. В работе предлагается усовершенствование существующей системы фрод-мониторинга, предназначенной для оценки финансовых и нефинансовых событий на предмет их подозрительности с точки зрения возможного мошенничества. Проведен анализ типового устройства антифрод-системы банка, выявлены его недостатки. Предложена новая структуры антифрод-системы с генеративным искусственным интеллектом, а также сформулированы основные риски использования такого подхода, а также меры по их недопущению и исправлению.
Ключевые слова: антифрод-система, генеративный искусственный интеллект, обнаружение и предотвращение финансовых мошенничеств

Введение

В банковской сфере всё чаще наблюдаются случаи, когда клиенты добровольно отправляют деньги третьим лицам, не подозревая при этом, что данные операции происходят с совершением обмана или злоупотреблением их собственного доверия, что приводит к значительным финансовым потерям как для них самих, так и для банков. Эффективное управление процессом обнаружения и предотвращения мошеннических операций позволяет минимизировать издержки и улучшить качество обслуживания клиентов [1– 4]. Актуальность данного исследования обусловлена значительным ущербом, который мошенничество наносит как отдельным финансовым организациям, так и экономикам стран в целом. Развитие цифровых технологий усиливает не только возможности для пользователей, но и потенциал для различных видов фрод-активностей, что делает борьбу с ними особенно актуальной.

Целью работы является разработка новой модели автоматизированного фрод-мониторинга для банка, которая позволит усовершенствовать процесс выявления и предотвращения мошеннических операций, сокращая риски и потери финансовых средств компании, за счет внедрения в неё генеративного искусственного интеллекта.

Методы

Методы исследования включают анализ тематической литературы, изучение практик в области фрод-мониторинга, проведение социологического исследования, а также сравнительного анализа и тестирования новых технологических решений.

Результаты и обсуждения

Анализ нормативно-правовой базы банковской отрасли Российской Федерации

Федеральный закон от 2 декабря 1990 года № 395–1 «О банках и банковской деятельности» является основополагающим нормативным актом, регламентирующим создание и функционирование кредитных организаций в Российской Федерации [5]. Этот закон устанавливает правовые основы деятельности банков и других кредитных организаций на территории РФ.

Согласно данному закону, банк представляет собой коммерческую организацию, обладающую правом на осуществление банковских операций, включая привлечение денежных средств от физических и юридических лиц во вклады, размещение привлечённых средств от своего имени и за свой счёт, открытие и ведение банковских счетов, проведение расчётов по поручению клиентов, инкассацию денежных средств, векселей и других платёжных документов, а также осуществление других операций.

Закон также устанавливает требования к минимальному размеру уставного капитала банков, регулирует вопросы лицензирования банковской деятельности, определяет порядок создания и ликвидации банков, а также устанавливает ответственность за нарушение банковского законодательства. Важно отметить, что закон определяет понятие кредитной организации (КО), включающее банки, небанковские кредитные организации и иностранные банки.

Федеральный закон от 27 июня 2011 года № 161-ФЗ устанавливает правовые и организационные основы национальной платёжной системы, регулирует порядок оказания платёжных услуг, включая переводы денежных средств и использование электронных платёжных средств [6]. Закон определяет требования к организации и функционированию платёжных систем, а также порядок надзора и контроля за их деятельностью.

Национальная платёжная система обеспечивает проведение платежей и других финансовых операций внутри страны. В России существуют несколько национальных платёжных систем, включая Национальную систему платёжных карт (НСПК), которая является операционным и платёжным клиринговым центром для обработки операций по банковским картам внутри России и оператором национальной платёжной системы «Мир».

Основные требования данного закона включают:

1. Регистрация операторов платёжных систем, платёжных агентов и операторов электронных денежных средств в Банке России и соблюдение установленных правил.
2. Соблюдение участниками платёжных систем правил безопасности и конфиденциальности информации о денежных переводах. Закон также регулирует меры по предотвращению мошенничества в сфере электронных платежей.

Федеральный закон «О персональных данных» регулирует обработку, хранение и доступ к персональным данным в России [7]. Он определяет ключевые понятия и требования, касающиеся персональных данных, таких как обработка, оператор, субъект персональных данных, конфиденциальность и согласие на обработку.

Основные положения закона включают следующие пункты:

1. Операторы, такие как банки, обязаны получать согласие на обработку персональных данных.
2. Обеспечение конфиденциальности данных и защита от несанкционированного доступа.
3. Уведомление субъектов о целях обработки данных и их правах.
4. Соблюдение требований при передаче данных за пределы РФ.

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает требования к защите информации и информационных технологий, что связано с борьбой с киберпреступностью [8]. Закон предписывает операторам информационных систем обеспечивать защиту данных от несанкционированного доступа, изменения и уничтожения, а также предусматривает ответственность за нарушение этих требований.

Федеральный закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» регулирует

меры, направленные на предотвращение и выявление операций, связанных с отмыванием доходов и финансированием терроризма [9]. Закон требует от банков и других кредитных организаций проведения идентификации клиентов, проверки на причастность к террористической деятельности и сообщения о подозрительных операциях соответствующим органам.

Анализ нормативно-правовой базы банковской отрасли Республики Узбекистан

Закон Республики Узбекистан, от 25.04.1996 г. № 216-I 1 «О банках и банковской деятельности» устанавливает правовые и организационные основы банковской сферы [10]. Этот документ определяет основные понятия и формулирует требования к субъектам данной отрасли Республики Узбекистан, регулирует банковскую деятельность.

Согласно данному закону, банком является юридическое лицо, являющееся коммерческой организацией и осуществляющее совокупность следующих видов деятельности: принятие вкладов от юридических и физических лиц и использование принятых средств для кредитования или инвестирования на собственный страх и риск; осуществление платежей.

Закон определяет условия создания банков, лицензирования и прекращения банковской деятельности, требования к величине и источников формирования уставного капитала, основания для отказа в регистрации банков и выдаче лицензии, основания для отзыва лицензии на проведение банковских операций, формулирует права и обязанности банков.

Закон Республики Узбекистан от 04.04.2006 г. № ЗРУ-30 «О защите информации в автоматизированной банковской системе» [11]. Он регулирует отношения в области защиты информации в автоматизированной банковской системе, определяет обязанности собственника автоматизированной банковской системы и требования к службе защиты информации.

Основные положения закона включают следующие пункты:

1. Собственник автоматизированной банковской системы обязан обеспечить защиту информации, согласно правилам, установленным Центральным банком Республики Узбекистан, и обязан уведомлять собственника информации обо всех фактах нарушения защиты его информации.
2. Собственник автоматизированной банковской системы обязан обеспечить защиту информации, содержащей государственные секреты или являющейся конфиденциальной, в порядке, установленном Кабинетом Министров Республики Узбекистан.
3. Служба защиты информации в автоматизированной банковской системе организует контроль за обеспечением сохранности информации, принимает меры по защите информации в автоматизированной банковской системе при выявлении попыток несанкционированного доступа к информации, других форм вмешательства и при нарушении правил функционирования системы.

Постановление Президента Республики Узбекистан, от 30.11.2023 г. № ПП-381 о мерах по усилению защиты прав потребителей цифровой продукции (услуг) и борьбы с правонарушениями, совершаемыми посредством цифровых технологий [12]. Основной целью постановления являются разработка единых требований

кибербезопасности для всех электронных платежных систем и строгий контроль за соблюдением этих правил. Документ вводит дополнительные требования к созданию и осуществлению деятельности операторов платежных систем и платежных организаций.

Основные положения постановления включают следующие пункты:

1. В целях своевременного пресечения краж, мошенничества и других правонарушений Центральный банк уполномочен направлять обязательные указания коммерческим банкам, операторам платежных систем и платежным организациям о временном ограничении использования на срок до трех дней банковских карт, банковских счетов и счетов на мобильных приложениях в случае осуществления сомнительных (фрод) операций, связанных с банковскими картами.

2. Центральный банк совместно с заинтересованными ведомствами обязан разработать и утвердить комплекс мер, предусматривающих:

- совершенствование методов технической защиты при оказании гражданам онлайн-услуг коммерческими банками, операторами платежных систем и платежными организациями, внедрение антифрод-систем, автоматизацию контроля осуществленных подряд трех и более переводов, внедрение механизмов контроля использования банковских карт и осуществления денежных переводов между физическими лицами в крупном размере с использованием дополнительных биометрических и иных мер защиты;
- повышение цифровой финансовой грамотности населения по предупреждению современных угроз, в частности незаконных операций с банковскими картами (их реквизитами), в том числе посредством электронных платежных систем.

Анализ статистических данных Российской Федерации

Согласно информации, предоставленной Центральным Банком Российской Федерации [13–14], в 2023 году наблюдалось увеличение объема незаконных операций, совершенных без согласия клиентов, на 11,48% по сравнению с предыдущим годом. Основным методом, используемым злоумышленниками для хищения средств, остается социальная инженерия. Эти виды операций составили 50,4% всех случаев, что демонстрирует рост по сравнению с предыдущим периодом.

Социальная инженерия представляет собой метод манипуляции, при котором злоумышленники используют психологические приемы для получения конфиденциальной информации или доступа к личным данным. Этот метод активно применяется мошенниками для совершения преступных действий и обмана клиентов банков [15].

Потерпевшими от финансового мошенничества может стать любой человек, вне зависимости от возраста и социального статуса. Однако, опрос Банка России позволил выделить среднестатистический портрет наиболее уязвимого клиента:

- Возраст от 25 до 44 лет.
- Проживает в городе.
- Мужчина со средним уровнем дохода и средним образованием.
- Активный пользователь банковских онлайн-сервисов.

Анализ статистических данных Республики Узбекистан

Согласно статистической информации, количество преступлений в сфере информационных технологий, совершенных в 2020 году в Узбекистане, составило 106, в 2021 году – 2281 [16]. В 2023 году этот показатель вырос более чем в 2 раза. 70% всех киберпреступлений составляют мошенничество и кражи, связанные с банковскими картами.

Основными способами, которые используют мошенники для кражи средств с карт являются:

- 34% — мошенники отправляют своим жертвам поддельные ссылки с предложениями финансовой помощи, получения онлайн-кредита или выигрышей, тем самым, получая секретный код или номер банковской карты;
- 22% — мошенники получают авансовые платежи, а после не выполняют оговоренные соглашения;
- 17% — мошенники представляются сотрудниками платежных компаний (Click, Payme и др.) или службы безопасности банка во время телефонных разговоров. Таким образом, они получают номера банковских карт или секретные коды;
- 14% — мошенники раскрывают секретный код или номер банковской карты через торговые онлайн-площадки;
- 9% — преступления совершаются через финансовые онлайн-биржи (Binance и др.)

Особенности антифрод-систем (АФС) банков

Фрод (fraud) представляет собой намеренные действия или бездействие физических и/или юридических лиц с целью получения выгоды за счет организации и/или нанесения ей материального и/или нематериального ущерба [17]. Система фрод-мониторинга включает в себя этапы обзора, обнаружения и предотвращения мошеннических операций. Согласно Кембриджскому словарю, "anti-fraud" означает направленный на предотвращение или уменьшение мошенничества или связанный с работой по предотвращению или уменьшению мошенничества [18]. Антифрод-системы (АФС) проверяют каждую транзакцию в режиме реального времени и блокируют те, которые не соответствуют установленным критериям.

Технология фрод-мониторинга использует комбинацию искусственного интеллекта (ИИ), машинного обучения и систем на основе правил для анализа операций. Искусственный интеллект в обнаружении мошенничества использует алгоритмы, которые отслеживают входящие данные и предотвращают угрозы мошенничества до их реализации. ИИ обучается на исторических данных и способен изменять свои правила для остановки новых угроз, с которыми он ранее не сталкивался. Это дает ему преимущество перед стандартным программным обеспечением для борьбы с мошенничеством. Такие системы учитывают различные данные, эффективно создавая «профиль» мошеннической деятельности на основе действий человека. Этот профиль затем используется для идентификации подозрительного поведения, которое необходимо исследовать.

Большинство решений для фрод-мониторинга работают непрерывно, в режиме реального времени, что критически важно для предотвращения мошенничества. Эти системы обычно интегрируются с различными бизнес-системами через программный интерфейс (API).

Существует множество стратегий, направленных на снижение уязвимости клиентов банков к психологическим атакам мошенников: биометрическая аутентификация, анализ поведения пользователя (User Behavior Analysis), мониторинг транзакций (Transaction Monitoring), система управления рисками (Risk Management System) и т.д. Их целью являются повышение точности отбора транзакций для отклонения и разработка сценариев воздействия на мошенников. Каждый из этих методов имеют свои плюсы и минусы. По мнению авторов, наиболее перспективным подходом является непосредственное воздействие на клиентов, что достигается путем использования метода анализа поведения пользователя (User Behavior Analysis). При данном подходе исследуется поведение пользователя на сайте или в приложении банка для определения подозрительной активности. Например, если пользователь внезапно начинает совершать большое количество транзакций или совершает операции в необычное время, это может служить индикатором мошенничества.

Для разработки эффективной стратегии противодействия мошенничеству был рассмотрен стандартный сценарий функционирования антифрод-системы. На первом этапе осуществляется внедрение мошенника в жизнь клиента через различные методы. Это означает, что мошенник каким-либо образом вступает во взаимодействие с клиентом, используя как прямые, так и косвенные методы воздействия. Ключевым моментом является реакция клиента на действия мошенника. В данном анализе исключены сценарии, при которых клиент не реагирует на мошеннические действия.

Согласно статистическим данным [19] наиболее частыми действиями, приводящими к утрате денежных средств клиентами, являются:

- посещение подозрительных веб-сайтов;
- открытие вкладки перевода средств;
- попытка снятия наличных;
- открытие полученного уведомления.

Стандартная антифрод-система на базе технологий искусственного интеллекта анализирует действия, совершаемые клиентом, и оценивает их на предмет соответствия привычному поведению. В зависимости от этой оценки система классифицирует операции как допустимые, сомнительные или недопустимые, передавая соответствующую метку платежной системе.

На данном этапе не предпринимаются непосредственные меры противодействия — система лишь присваивает потенциальным операциям соответствующие метки: одобрить, проверить или заблокировать. Зеленые метки означают, что всё в порядке, желтые указывают на необходимость дополнительной проверки, а красные метки сигнализируют о мошенничестве. После присвоения метки система фрод-мониторинга уведомляет платежную систему, которая решает, что делать с транзакцией. Например, транзакции с желтой меткой потребуют дополнительного подтверждения, а красные транзакции блокируются. Эти операции остаются потенциальными, поскольку клиент может не завершить их после совершения первого действия.

Важно разграничивать понятия «совершенное действие» и «совершенная операция»: пока клиент не перевел средства, а лишь совершил некоторые действия, такие как посещение подозрительного сайта, это считается «совершенным действием». В свою очередь, когда клиент уже перевел средства или оплатил покупку,

введя специальный код, это рассматривается как «совершенная операция». Таким образом, возможны два сценария: клиент либо отказывается от совершения операции, либо завершает её.

Если клиент отказывается от операции, его средства остаются неприкосновенными. Однако, если клиент решает продолжить операцию, автоматизированная АФС снова активируется, задействуя механизм превенции. Если операция проходит установленные фильтры, АФС помечает её как допустимую, и клиент теряет деньги. В случае несоответствия определённым фильтрам, АФС классифицирует операцию как сомнительную или недопустимую и передает эту информацию в платёжную систему. Сомнительные операции подвергаются дополнительным проверкам с применением дополнительных фильтров, и чаще всего переходят в категорию недопустимых. В итоге платёжная система блокирует такие операции. После блокировки сотрудник банка связывается с клиентом, объясняя причину отказа в проведении операции и давая рекомендации по дальнейшим действиям. Схема всего процесса представлена на рисунке 1.

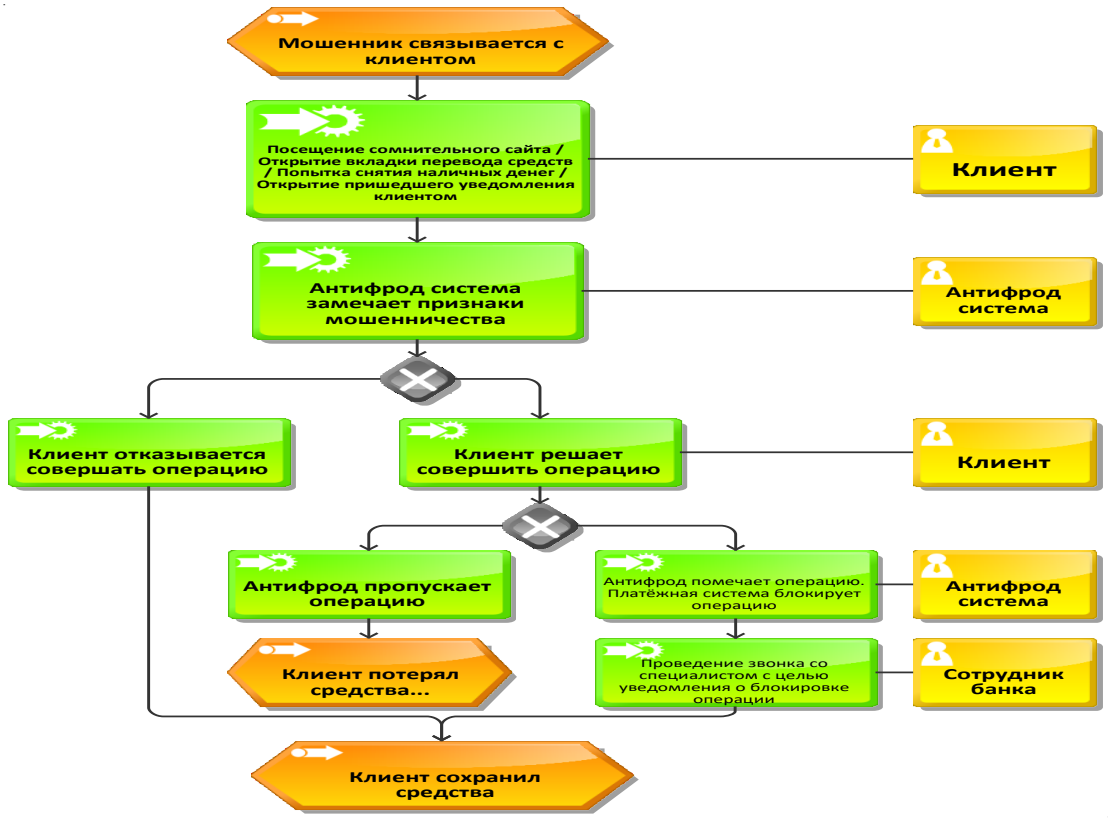

Рис. 1. Схема процесса типовой антифрод-системы банка

Анализ полной схемы процесса позволяет выявить основные проблемные этапы. Во-первых, хотя АФС задействуется еще до совершения операции, на этом этапе она не влияет на окончательный результат, несмотря на затраты производственных мощностей. Это действие оправдано необходимостью подготовки системы к возможной операции клиента, но для повышения эффективности системы важно информировать клиента о потенциальных рисках мошенничества сразу после выявления признаков мошеннической активности.

Кроме того, на завершающем этапе, когда операция отклоняется, сотрудник банка должен связаться с клиентом для объяснения причины отказа. Чтобы избежать путаницы, сотрудник сначала должен понять, какие именно действия клиента привели к блокировке. Это требует дополнительных временных затрат и может стать дополнительным стрессовым фактором для клиента в таких ситуациях.

Антифрод-система с использованием генеративного ИИ

В данном исследовании авторами предлагается внедрение генеративного искусственного интеллекта в систему анализа поведения пользователей (User Behavior Analysis) банка. Генеративный ИИ будет способен генерировать текстовые уведомления и аудиосообщения для клиентов.

При обнаружении подобной системой потенциальных мошеннических действий она будет автоматически отправлять уведомления через мобильное приложение банка, предупреждая клиентов о возможных угрозах и предлагая меры по усилению безопасности. Например, если ИИ выявляет необычные или подозрительные транзакции, клиенту будет направлено предупреждение о возможном мошенничестве с рекомендацией изменить пароль или включить двухфакторную аутентификацию.

Внедрение генеративного искусственного интеллекта позволит значительно уменьшить количество мошеннических атак, повысить уровень безопасности и защитить клиентов от финансовых потерь.

Генеративный искусственный интеллект — это технология, позволяющая компьютеру создавать новый контент на основе заложенных данных. Генеративные модели ИИ могут создавать тексты, изображения, музыку, видео и другие виды контента, анализируя большие объемы данных и выявляя закономерности для генерации новых материалов.

Схема усовершенствованного процесса с генеративным ИИ представлена на рисунке 2.

Таким образом, если уже на начальном этапе антифрод-система обнаруживает признаки мошеннической активности, она сразу же будет генерировать и отправлять клиенту в мобильном приложении банка предупреждающее уведомление о подозрительной ситуации. Впоследствии система создаст сценарий взаимодействия с клиентом, разъясняя, что именно вызывает подозрения, какие действия предшествовали этому и какие меры рекомендуется предпринять. Дополнительно система создаст виртуального банковского сотрудника, адаптированного под предпочтения клиента. Если клиент не отреагирует на уведомление, виртуальный помощник самостоятельно свяжется с ним. Генеративный ИИ обладает способностью озвучивать текст в реальном времени, что минимизирует риск временных задержек.

Риски использования обнаружения мошенничества с помощью ИИ

Существуют несколько ключевых рисков, связанных с использованием ИИ в современных банковских системах.

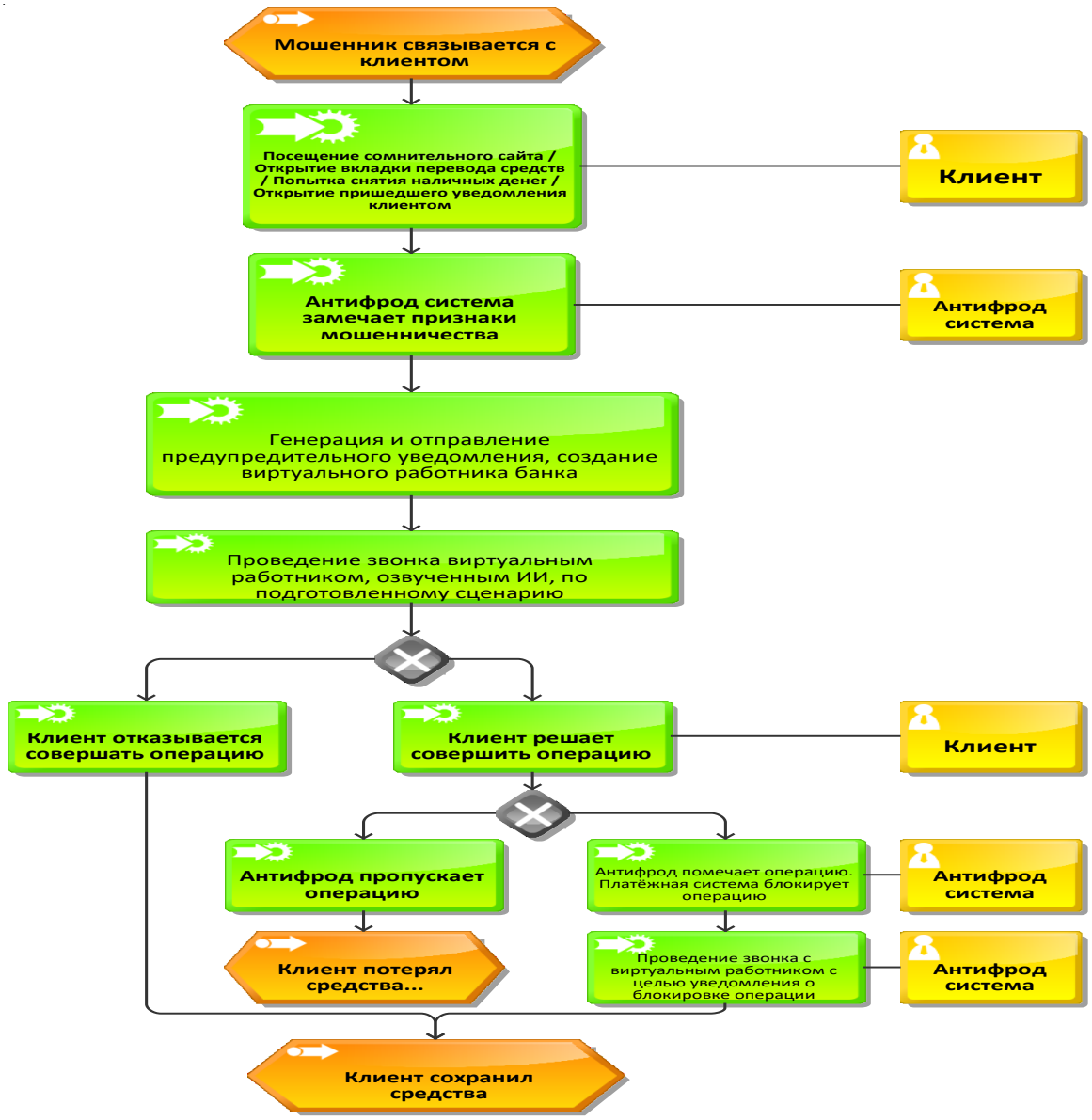

Рис. 2. Предлагаемый процесс работы антифрод-системы, улучшенный генеративным искусственным интеллектом

• Сложность интерпретации работы ИИ: поскольку ИИ обрабатывает огромные объемы данных, зачастую сложно понять его внутренние механизмы. Это особенно актуально для систем, использующих машинное обучение и нейронные сети, имитирующие человеческий мозг. Однако передовое программное обеспечение для обнаружения мошенничества предоставляет разнообразные инструменты для настройки его правил в соответствии с требованиями банка.

• Ложные срабатывания: несмотря на то, что ИИ значительно сокращает количество ложных срабатываний, их полное исключение невозможно. Периодически ИИ будет блокировать законных пользователей, особенно тех, кто использует нестандартные браузеры и VPN.

• Социальное мошенничество: Этот вид мошенничества трудно обнаружить с помощью ИИ. Один поддавшийся уловке сотрудник может поставить под угрозу безопасность всей компании. Поэтому необходимо регулярно обучать сотрудников методам противодействия таким угрозам.

• Предвзятость алгоритмов: Алгоритмы могут демонстрировать предвзятость по отношению к людям определенного пола, этнической или религиозной принадлежности.

В исследовании выявлены несколько значительных рисков, связанных с использованием генеративного искусственного интеллекта, а также сформулированы меры по их предотвращению и избавлению в случае возникновения. Данные представлены в таблице 1.

Таблица 1

Риски при использовании генеративного ИИ

Риск	Способ предотвращения	Способы избавления в случае возникновения
Неточности в генерации пользовательских данных	Регулярное обновление и тестирование моделей ИИ	Корректировка данных и пересоздание профилей пользователей
Искажение персонализированных предложений	Настройка алгоритмов на основе точных данных о клиентах	Пересмотр алгоритмов и обновление данных предложений
Проблемы с конфиденциальностью данных	Использование шифрования и строгих политик доступа к данным	Уведомление пользователей и принятие мер по усилению безопасности
Создание неприемлемого контента	Фильтрация и мониторинг генерируемого контента	Удаление неприемлемого контента и извинение перед пользователями
Социальное мошенничеств	Обучение сотрудников и клиентов распознаванию мошеннических схем	Проведение внутреннего расследования и обучение персонала
Недостаточная прозрачность работы ИИ	Предоставление объяснений и отчетов по работе ИИ	Проведение аудитов и анализов для улучшения прозрачности работы ИИ

Выводы и рекомендации

В ходе исследования были выявлены ключевые проблемы типовой антифрод-системы и определена необходимость оптимизации процессов. Основные проблемы включали повышенную уязвимость клиентов к приёмам социальной инженерии и недостаточную осведомленность клиентов о мошеннических схемах.

В рамках сравнительного анализа рассматривались различные методы: улучшение системы фильтрации операций, прямое противодействие мошенникам и использование генеративного искусственного интеллекта, основанного на методе анализа поведения пользователя (User Behavior Analysis). В результате было принято решение о внедрении генеративного искусственного интеллекта, так как этот метод наиболее эффективно устраняет выявленные проблемы. Тестирование системы показало, что внедрение генеративного ИИ позволяет существенно улучшить показатели количества отраженных атак и уровень баланса наличности по сравнению с текущей моделью.

Научная ценность работы заключается в разработке новой модели антифрод-системы, основанной на использовании передовых технологий искусственного

интеллекта. Эта модель усовершенствовала процесс выявления и предотвращения мошеннических операций, сокращая риски и потери финансовых средств банка за счет внедрения генеративного искусственного интеллекта.

Результаты исследования могут быть использованы для модернизации систем безопасности в банках и других финансовых учреждениях.

Список литературы

1. Исаева П.Г. Османова С.М. Структура коммерческого банка и организационные основы его деятельности / П.Г. Исаева, С.М. Османова // Azimuth of Scientific Research: Economics and Administration. – 2020. – №2. (31). – С. 262-265.
2. Чеботарева Г.С. Организация деятельности коммерческого банка Екатеринбург: Издательство Уральского университета. – 2018. – С. 122.
3. Клейман Н.А. Совершенствование организационной структуры коммерческого банка с учетом принципов реквизитной организации на примере ПАО КБ "УБРиР»: магистерская диссертация / Н.А. Клейман; УРФУ им. Б. Н. Ельцина, Институт экономики и управления, Кафедра систем управления энергетикой и промышленными предприятиями. – Екатеринбург, 2018. – 83 с.
4. Бородин А.И. и др. Банковский менеджмент. Учебник. Т. 3. / Под ред. Ю.А. Ровенского, Ю.Ю. Русанова. – М., Проспект, 2017. – 384 с.
5. https://www.consultant.ru/document/cons_doc_LAW_5842/
6. https://www.consultant.ru/document/cons_doc_LAW_115625/
7. https://www.consultant.ru/document/cons_doc_LAW_61801/
8. https://www.consultant.ru/document/cons_doc_LAW_61798/
9. https://www.consultant.ru/document/cons_doc_LAW_32834/
10. https://lex.uz/docs/12011
11. https://lex.uz/docs/974160
12. https://lex.uz/uz/docs/6681115
13. Банк России [Электронный ресурс] // cbr.ru. URL: https://www.cbr.ru/analytics/ib/operations_survey/2023/ (дата обращения: 15.02.2024).
14. Банк России [Электронный ресурс] // cbr.ru. URL: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 14.01.2024).
15. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений / М.О. Янгаева // Вестник Сибирского юридического института МВД России. – 2021. – №1 (42). – С. 133-138.
16. https://uz.kursiv.media/2023-12-20/v-2023-m-v-uzbekistane-bylo-sovershenо-55-tys-kiberprestuplenij/
17. Киселев И.И., Одинцова С.А. Автоматизация процессов фрод-мониторинга транзакций коммерческого банка / И.И. Киселев, С.А. Одинцова // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – №5 – С. 4206-4215.
18. Кембриджский словарь Cambridge dictionary [Электронный ресурс] // dictionary.cambridge.org. URL.: https://dictionary.cambridge.org/dictionary/english/anti-fraud (дата обращения: 18.05.2024).
19. Портал статистики и рыночных данных «Statista» [Электронный ресурс] // statista.com URL.: https://www.statista.com/statistics/786778/worldwide-fraud-detection-and-prevention-market-size/ (дата обращения: 10.02.2024).]