Мардонов Амиржон Шерзод угли,
преподаватель кафедры «Кибер право», ТГЮУ
Email: amirmardonov39@gmail.com
ORCID: https://orcid.org/0009-0004-8116-8370

ПРАВОВЫЕ МЕХАНИЗМЫ УПРАВЛЕНИЯ РИСКАМИ ПРИ ПРИМЕНЕНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ БАНКОВСКОГО СКОРИНГА

Аннотация. В статье рассматриваются правовые механизмы управления рисками при внедрении систем искусственного интеллекта (ИИ) в банковский скоринг. Проанализированы международные стандарты и подходы – GDPR**,** проект Регламента ЕС об ИИ (EU AI Act), стандарт ISO/IEC 23894:2023 – а также законодательство Республики Узбекистан (Закон «О персональных данных», Стратегия развития ИИ до 2030 года и др.). На основе сравнительного анализа и изучения кейсов (Apple Card в США, SCHUFA в Германии, Asia Alliance Bank в Узбекистане) выявлены ключевые риски применения ИИ в кредитном скоринге: дискриминация, непрозрачность алгоритмов, нарушение прав потребителей и неадекватность моделей. Рассматриваются существующие правовые меры для минимизации данных рисков, такие как требования по недопущению **алгоритмической дискриминации**, обеспечение прозрачности и объяснимости решений, защита персональных данных и права потребителей на обжалование автоматизированных решений. В разделе обсуждения предложены рекомендации по совершенствованию регулирования использования ИИ в сфере банковского кредитования в Узбекистане с учётом международного опыта – включая разработку специальных нормативных актов по высокорисковым ИИ-системам, обязательное проведение оценок рисков и аудитов алгоритмов, усиление надзора за соблюдением принципов справедливости и прозрачности. Реализация данных мер позволит уменьшить вероятность алгоритмических ошибок и злоупотреблений, повысить уровень доверия к ИИ-системам в финансовом секторе и обеспечить баланс между инновациями и защитой прав граждан.

Ключевые слова: искусственный интеллект, кредитный скоринг, алгоритмический риск, дискриминация, прозрачность, регулирование и персональные данные.

Mardonov Amirjon Sherzod o‘g‘li
TDYU “Kiber huquq” kafedrasi o‘qituvchisi
Email: amirmardonov39@gmail.com
ORCID: https://orcid.org/0009-0004-8116-8370

BANK SKORINGI TIZIMIDA SUN’IY INTELLEKTNI QO‘LLASHDA XAVFLARNI BOSHQARISHNING HUQUQIY MEXANIZMLARI

Annotatsiya. Maqolada bank kredit skoringida sun’iy intellekt (SI) tizimlarini joriy etishda xavflarni boshqarishning huquqiy mexanizmlari ko‘rib chiqilgan. Xalqaro standartlar va yondashuvlar — GDPR, Yevropa Ittifoqining SI to‘g‘risidagi reglamenti (EU AI Act) loyihasi, ISO/IEC 23894:2023 standarti hamda O‘zbekiston Respublikasining qonunchiligi («Shaxsiy ma’lumotlar to‘g‘risida»gi Qonun, 2030 yilgacha SIni rivojlantirish strategiyasi va boshqalar) tahlil qilingan. Solishtirma tahlil va keyslar (Apple Card — AQSH, SCHUFA — Germaniya, Asia Alliance Bank — O‘zbekiston) asosida SIni kredit skoringida qo‘llashning asosiy xavflari aniqlangan: diskriminatsiya, algoritmlarning shaffof emasligi, iste’molchilar huquqlarining buzilishi va modellar muvofiqsizligi. Mavjud huquqiy choralar tahlil qilingan, jumladan,

algoritmik diskriminatsiyaga yo‘l qo‘ymaslik, qarorlarning shaffofligi va tushunarliligini ta’minlash, shaxsiy ma’lumotlarni himoya qilish va avtomatlashtirilgan qarorlarga shikoyat qilish huquqi. Muhokama bo‘limida xalqaro tajribani hisobga olgan holda O‘zbekistonda bank kreditlash sohasida SIdan foydalanishni tartibga solishni takomillashtirish bo‘yicha takliflar berilgan — yuqori xavfli SI tizimlari uchun maxsus normativ hujjatlar ishlab chiqish, xavflarni baholash va algoritmlarni auditdan o‘tkazish majburiyati, adolat va shaffoflik tamoyillariga rioya etilishini kuchaytirish. Ushbu choralar SI tizimlarida algoritmik xatolar va suiiste’molchilik xavfini kamaytirishga, moliya sohasida ishonchni oshirishga va fuqarolar huquqlarini himoya qilish bilan innovatsiyalar o‘rtasida muvozanat ta’minlashga xizmat qiladi.

Kalit so‘zlar: sun’iy intellekt, kredit skoring, algoritmik xavf, diskriminatsiya, shaffoflik, tartibga solish va shaxsiy ma’lumotlar.

ВВЕДЕНИЕ

Активное внедрение технологий искусственного интеллекта в банковской сфере открывает новые возможности для повышения эффективности и доступности финансовых услуг. Одним из ключевых примеров является использование алгоритмов машинного обучения [1] для кредитного скоринга – автоматизированной оценки платёжеспособности заемщиков. ИИ-модели способны оперативно анализировать большие объемы данных и выявлять сложные корреляции, что потенциально повышает точность прогнозирования кредитных рисков и расширяет доступ к кредитам для клиентов без кредитной истории. Однако наряду с этими преимуществами применение ИИ несёт и серьёзные риски. Исследования и практика показывают, что алгоритмы скоринга могут страдать от системной предвзятости (bias), приводящей к дискриминации определённых групп заемщиков, работать как «чёрный ящик» без прозрачного объяснения принятого решения, а также нарушать права потребителей – в частности, право на неприкосновенность персональных данных и справедливое рассмотрение заявки [2].

В последние годы получили огласку резонансные случаи, подчеркнувшие реальность указанных рисков. Так, в 2019 г. алгоритм кредитного скоринга, используемый Apple Card (совместный проект Apple и Goldman Sachs), подвергся обвинениям в гендерной дискриминации [3]: известные ИТ-специалисты сообщили, что кредитные лимиты их жен были в разы ниже, чем у них самих при прочих равных финансовых показателях. Эта ситуация вызвала широкий общественный резонанс и привела к началу расследования регуляторами финансового рынка Нью-Йорка. Другой пример – деятельность немецкого кредитного бюро SCHUFA [4], чья закрытая модель расчёта кредитного рейтинга критиковалась за непрозрачность и возможную несправедливость. В 2023 г. по делу клиента SCHUFA Суд ЕС вынес прецедентное решение о том, что полностью автоматизированное присвоение кредитного балла, существенно влияющего на возможность получения займа, подпадает под запрет статьи 22 GDPR. Компания SCHUFA, ссылаясь на коммерческую тайну, отказывалась раскрыть клиентам детали алгоритма и учитываемые факторы, что породило дискуссию о конфликте между правом на информацию и защитой ноу-хау.

Возникает научно-практический вопрос: **какими правовыми средствами можно управлять рисками алгоритмического скоринга** [5], чтобы максимально использовать преимущества ИИ в кредитовании, минимизируя сопутствующие угрозы? В разных юрисдикциях уже формируются подходы к регулированию ИИ-систем. Европейский союз в рамках комплексного **риско-ориентированного подхода** [6] планирует ввести специальные требования для «систем высокого риска», к которым отнесены и алгоритмы оценки кредитоспособности. Международные организации по стандартизации разрабатывают руководства по **управлению рисками ИИ** [7] (например, недавно опубликован стандарт ISO/IEC 23894:2023). В Узбекистане действует законодательство о персональных данных, частично затрагивающее вопросы автоматизированных решений, и принята Стратегия развития ИИ, намечающая шаги по развитию и регулированию данной сферы. **Целью исследования** является анализ и сравнение правовых механизмов, направленных на идентификацию и минимизацию рисков при применении искусственного интеллекта в системе банковского скоринга.

МЕТОДОЛОГИЯ И МАТЕРИАЛЫ.

Исследование выполнено по схеме **сравнительного правового анализа** (comparative analysis) [8]. В качестве основных объектов сравнения выбраны регуляторные подходы Европейского союза (как региона, активно внедряющего специальные нормы об ИИ) и Республики Узбекистан (как государства, где применение ИИ-технологий в финансах находится в начальной стадии развития). Анализ международных стандартов проводится преимущественно на материале права ЕС и рекомендаций профильных организаций. Рассмотрены нормативные акты: Общий регламент ЕС о защите данных 2016/679 (далее – GDPR) [9] – в части ограничений автоматизированного принятия решений; проект Регламента ЕС «Об искусственном интеллекте» – в части требований к высокорисковым ИИ-системам; международный стандарт ISO/IEC 23894:2023 «Artificial intelligence — Guidance on risk management» – как свод лучших практик по управлению рисками ИИ. С узбекской стороны проанализированы Закон Республики Узбекистан «О персональных данных» №ЗРУ-547 от 02.07.2019 (особенно нормы об автоматизированной обработке данных), а также стратегические и программные документы (например, Постановление Президента РУз от 14.10.2024 №ПП-358, утвердившее Стратегию развития технологий ИИ до 2030 года).

РЕЗУЛЬТАТЫ.

GDPR устанавливает базовые рамки, влияющие на использование ИИ в скоринге, через призму защиты персональных данных и прав субъектов. Ключевое значение имеет **статья 22 GDPR**, которая предусматривает, что субъект данных имеет право не подвергаться решению, основанному исключительно на автоматизированной обработке, если оно производит для него юридические последствия или иным образом существенно затрагивает его права и законные интересы. Кредитный скоринг, определяющий

возможность выдачи займа, прямо подпадает под эту норму, что подтверждено Судом ЕС в деле OQ vs. SCHUFA (2023) [10] – **присвоение кредитного балла** признано автоматизированным решением, способным существенно влиять на права субъекта. GDPR не вводит полного запрета на такие решения, но разрешает их **только при соблюдении дополнительных условий** (ст.22(2)): когда автоматизированное решение необходимо для заключения или исполнения договора с субъектом, либо прямо разрешено законом, либо основано на явном согласии субъекта.

Следующим этапом развития европейского регулирования ИИ является готовящийся **Акт об искусственном интеллекте** (Artificial Intelligence Act) [11], представленный Еврокомиссией в 2021 г. (далее - AI Act). Это первый комплексный законопроект, специально посвященный ИИ. Он вводит классификацию систем ИИ по уровням риска и устанавливает наиболее строгие требования к так называемым системам высокого риска**.** Приложение III к проекту прямо относит системы, предназначенные для оценки кредитоспособности физических лиц или для установления их кредитного рейтинга, к категории высокорисковых (раздел 5(b) Annex III).

Перед вводом в эксплуатацию поставщик высокорисковой системы ИИ должен пройти оценку соответствия всем этим требованиям и получить маркировку CE, подтверждающую безопасность/легальность продукта для рынка ЕС. Непосредственно для банков-пользователей AI Act также накладывает обязанности – эксплуатировать систему в соответствии с инструкцией, мониторить ее работу и сообщать о серьезных инцидентах регуляторам. Таким образом, будущий европейский режим является **проактивным** – он стремится заранее встроить механизмы управления рисками (от этапа разработки до применения), особенно против **дискриминации и непрозрачности**. Хотя AI Act еще не вступил в силу (ожидается окончательное утверждение в 2024–2025 гг.), многие эксперты отмечают, что он станет образцом для других стран при создании аналогичных правил.

В сфере «мягкого права» важным ориентиром служат международные стандарты. В 2023 году Международная организация по стандартизации (ISO) совместно с Международной электротехнической комиссией (IEC) выпустила первый специальный стандарт, посвящённый рискам ИИ – **ISO/IEC 23894:2023 «Artificial Intelligence – Guidance on Risk Management»** [12]. Этот документ не носит обязательного характера, но предлагает организациям систематический подход к выявлению и минимизации рисков при создании и использовании систем ИИ. Стандарт включает основные принципы управления рисками (Clause 4), рамочную структуру risk-management (Clause 5) и описание процесса управления рисками применительно к ИИ (Clause 6). Для финансовых организаций, внедряющих ИИ-скоринг, ISO 23894 дает ряд полезных рекомендаций:

- Руководство организации должно признать специфические риски ИИ и встроить их мониторинг в общую систему **управления рисками** и внутреннего контроля. Речь идет о формировании политики по ИИ,

определении зон ответственности (назначение ответственных за этичность ИИ, создание комитетов по ИИ-рискам) и культуры, поддерживающей осознанное использование ИИ.

- Стандарт призывает учитывать риски не только при эксплуатации модели, но и на стадиях **проекта, разработки, тестирования и внедрения**. В частности, Annexes к стандарту содержат перечни типичных источников рисков в ИИ-системах – таких как **смещение данных (data bias)**, ошибки алгоритмов, риски кибербезопасности, нарушения конфиденциальности, юридические и регуляторные риски. Организация должна проанализировать, какие из этих рисков актуальны для конкретного приложения (например, для кредитного скоринга – риск дискриминации, утечки персональных данных, неверной классификации клиентов и др.), и **оценить их вероятности и последствия**.
- Для значимых рисков нужно планировать **мероприятия по снижению**: это может включать улучшение качества данных (отсеивание предвзятых признаков), введение автоматических и ручных проверок результатов модели, ограничение сфер применения алгоритма, обучение персонала правильной интерпретации выводов ИИ. Стандарт указывает на важность обеспечения **прозрачности и подотчетности** алгоритмов как одного из методов снижения риска. Также рекомендуется предусмотреть **план реагирования** на инциденты с участием ИИ (например, если выявлена скрытая дискриминация, есть процедура оперативного приостановления использования модели и разбирательства).
- Управление рисками должно быть **непрерывным процессом**. После внедрения скоринговой ИИ-системы банк обязан регулярно **отслеживать качество** ее решений, собирая статистику ошибок, жалоб клиентов, случаев неоднозначных результатов. По данным мониторинга необходимо периодически **пересматривать модель** – например, обновлять ее на новых данных, если обнаружено ухудшение точности или появление систематического перекоса. Отдельно подчёркивается готовность организации **отключить или модифицировать** алгоритм, если риски выйдут на недопустимый уровень.

Применение стандарта ISO 23894 само по себе не гарантирует решение всех проблем, но способствует созданию у разработчиков и пользователей ИИ осознанного отношения к возможным негативным эффектам. Отмечается, что основные риски ИИ в финансах – это усиление уже существующих перекосов данных, проблемы приватности и воспроизводства **системной дискриминации**. Например, если исторические данные кредитования отражают дискриминационные практики прошлого, то без специальных мер ИИ их унаследует и даже усугубит. Стандарт призывает выявлять такие латентные проблемы и устранять их до того, как они повлияют на результат работы алгоритма. Также подчеркивается, что совокупность правовых ограничений (GDPR и др.) требует учёта при разработке ИИ – несоответствие

им само по себе является риском (юридическим, репутационным). В целом ISO 23894:2023 обеспечивает методическую поддержку для реализации тех требований, которые закрепляются на уровне законодательства в ЕС. Банки, придерживающиеся этих рекомендаций, снижают вероятность столкнуться с регуляторными санкциями **и** этическими скандалами из-за ИИ-скоринга.

Закон «О персональных данных» и автоматизированный скоринг. Ключевым действующим актом, затрагивающим применение ИИ в обработке клиентских данных, является Закон Республики Узбекистан «О персональных данных» №ЗРУ-547 от 2 июля 2019 года [13]. Этот Закон, во многом основанный на моделях зарубежных законов о данных, также содержит нормы об автоматизированной обработке. В статье 24 прямо закреплено право субъекта на отказ от принятия решения, основанного исключительно на автоматизированной обработке его персональных данных, если такое решение затрагивает его права и законные интересы и влечет юридические последствия. Исключения аналогичны GDPR: автоматизированное решение допускается с письменного согласия субъекта; при заключении или исполнении договора с ним; либо в случаях, предусмотренных законодательством. Таким образом, заявитель на кредит в Узбекистане формально тоже защищён от полностью автоматического отказа – банк должен либо получить согласие на скоринг, либо предусмотреть участие человека. Важно отметить, что узбекский закон идёт чуть дальше GDPR в детализации гарантий: он обязывает владельца/оператора данных разъяснить субъекту порядок принятия решения на основе ИИ, его возможные правовые последствия, предоставить возможность заявить возражение, а также разъяснить порядок защиты субъектом своих прав**.** Эта норма фактически закрепляет право на информацию об алгоритме и на оспаривание решения. Более того, при поступлении возражения оператор обязан рассмотреть его и уведомить заявителя о результате в письменной форме в 10-дневный срок. Для сравнения, GDPR лишь общими словами говорит о «праве получить вмешательство человека» и «оспорить решение», тогда как Закон РУз прописывает конкретную обязанность оператора дать разъяснения и ответить на жалобу.

Важно учитывать, что контроль за соблюдением Закона о персональных данных осуществляет уполномоченный госорган – в настоящее время это *Государственный центр персонализации при Кабинете Министров* (ранее – Государственный инспектор по надзору в сфере информатизации). В случае жалоб потребителей на алгоритмический скоринг этот орган теоретически мог бы провести проверку банка и выдать предписание. Однако на 2025 г. прецедентов таких разбирательств в публичном поле не отмечено, что объясняется пока невысокой распространенностью автоматизированного скоринга и низкой осведомлённостью населения о своих правах в этой сфере.

14 октября 2024 г. Президент Республики Узбекистан утвердил **Стратегию развития технологий искусственного интеллекта до 2030 года** (ПП-358-сон) [14]. Этот программный документ, помимо задач развития ИИ-индустрии, содержит и ряд положений, касающихся **регулирования и**

управления рисками при применении ИИ. В частности, Стратегия провозглашает целью создание необходимых условий для широкого внедрения ИИ, включая **формирование правовых основ** и механизмов обеспечения безопасности. Для финансового сектора прямо предусмотрено заимствование международного опыта: Центральному банку и коммерческим банкам поручено внедрять ИИ-технологии в управление рисками, в том числе для оценки кредитоспособности клиентов на основе больших данных. Одновременно особый акцент сделан на **защите персональных данных** при использовании ИИ. Так, в плане реализации Стратегии поставлена задача разработки отдельного нормативно-правового акта, направленного на обеспечение безопасности персональных данных при внедрении и использовании ИИ, *с опорой на передовую международную практику* (срок – до мая 2025 г.). Это означает, что уже в ближайшее время в Узбекистане ожидается принятие подзаконного акта или поправок, конкретизирующих требования к обработке персональных данных именно в ИИ-системах (вероятно, речь будет о порядке анонимизации данных, проведении оценок воздействия на приватность при внедрении ИИ и т.п., по аналогии с подходами GDPR).

Кроме того, Стратегия учреждает Научно-исследовательский институт по развитию цифровых технологий и искусственного интеллекта (при Министерстве цифровых технологий) и указывает на его роль в экспертизе ИИ-систем. Все информационные системы и программное обеспечение на основе ИИ, внедряемые в стране, должны проходить **экспертную оценку** данного Центра. Это фактически вводит механизм предварительного контроля алгоритмов со стороны государства. Например, если банк захочет запустить новую скоринговую модель, он обязан будет предоставить ее в Центр ИИ на экспертизу. Предмет такой экспертизы – соответствие технологии установленным требованиям (вероятно, тем самым, что будут закреплены в новом акте о безопасности персональных данных при ИИ). Хотя конкретные методики проверки пока не опубликованы, можно предположить, что Центр будет оценивать, не нарушает ли модель права граждан, нет ли в ней явных ошибок или biais. Такой подход созвучен требованию **конформности** в AI Act, но реализуется силами национального института.

ОБСУЖДЕНИЕ.

Обобщая результаты анализа, можно выделить четыре основных **категории рисков** при использовании ИИ в банковском скоринге и оценить, насколько эффективно они покрываются существующими правовыми мерами, а также что ещё следует сделать.

Алгоритмы машинного обучения могут непреднамеренно унаследовать **систематические предубеждения**, присутствующие в исходных данных или возникшие из-за особенностей модели. В кредитовании это ведёт к **неравному обращению с разными группами клиентов** [15]. Например, как показал случай Apple Card, женщины могут получать менее выгодные условия кредита по сравнению с мужчинами при аналогичных финансовых показателях. Традиционное антидискриминационное законодательство (как в США и ЕС)

уже распространяется на такие ситуации, но его применение постфактум затруднено из-за сложности доказать причинно-следственную связь между работой алгоритма и фактом дискриминации. Инструменты GDPR (ст.5 – принцип справедливости обработки, ст.9 – запрет обработки чувствительных данных о расе, здоровье и т.д.) дают косвенную защиту, но прямого упоминания «алгоритмической дискриминации» нет. Проект AI Act восполняет этот пробел, требуя проверки датасетов и результатов на отсутствие смещения против защищенных групп. В национальном праве Узбекистана также отсутствуют нормы, прямо запрещающие bias модели, хотя Конституция и Закон «О гарантиях равных прав и возможностей женщин и мужчин» (2019 г.) декларируют равноправие.

Большинство ИИ-моделей, особенно глубокие нейронные сети, функционируют как «черный ящик» [16], выдавая результат без человечесочитаемого обоснования. Для заемщика (да и для кредитного офицера) это означает непонимание, почему отказано в кредите. Правовой аспект прозрачности отражен в нормах о **праве на информацию** [17]. GDPR и Закон РУз «О персональных данных» фактически дают человеку право узнать, по каким данным и по какой логике вынесено автоматическое решение. Однако реализация этого права сложна: как показать «логику» нейросети в понятной форме? На практике банки могут предоставлять общие причины: например, «недостаточный доход» или «неполная кредитная история». Этого может быть недостаточно для реальной прозрачности – клиент не способен проверить или опровергнуть такой вердикт. В кейсе SCHUFA видна крайность непрозрачности: под предлогом коммерческой тайны алгоритм практически **неконтролируем** извне. Необходимо искать баланс. Международный опыт предлагает несколько решений:

а) использовать методы **Explainable AI (XAI)** – специальные алгоритмы, которые строят наглядные объяснения к выводам сложной модели (например, определяют, сколько процентного влияния на скор скоринга оказали доход, долги, возраст и т.д.). В научных работах по XAI для кредитного скоринга демонстрируется, что это повышает доверие и позволяет выявить скрытые проблемы модели [18].

б) Закрепить регуляторно минимальный набор информации, предоставляемой клиенту при автоматическом отказе. Например, в США действует требование рассылать «Adverse Action Notice» с указанием до четырех основных причин отказа по данным кредитного отчета. В Узбекистане можно аналогично обязать банки информировать заемщика об основных факторах, повлиявших на отрицательное решение (например: «низкий кредитный рейтинг», «нестабильный доход» и т.п.) [19].

в) Усилить независимый надзор за алгоритмами: чтобы компенсировать невозможность полного раскрытия модели всем, регулятор или уполномоченный орган (например, создаваемый Центр ИИ) должны иметь доступ к информации о алгоритме. Если модель приобретена у внешнего вендора, банк обязан получить от него достаточные сведения и поделиться с регулятором при запросе. Это должно быть закреплено нормативно – в

лицензионных требованиях или в том специальном акте, что разрабатывается в развитие Стратегии.

Традиционно права заемщиков защищаются нормами о потребительском кредитовании, которые обязывают кредитора действовать добросовестно и предоставлять информацию. С появлением AI-систем возникло опасение, что клиенты могут сталкиваться с несправедливым решением и не иметь возможности его оспорить [20]. Именно поэтому законодательно введено право на человеческое вмешательство и обжалование автоматизированного решения (в GDPR и Законе о персональных данных РУз). Однако реальное упражнение этого права требует налаженного процессуального механизма. Банк должен иметь внутреннюю процедуру рассмотрения обращений по итогам скоринга: например, клиент, не согласный с отказом, подает заявление, после чего другой кредитный эксперт или комитет повторно оценивает заявку уже без участия ИИ либо с его участием, но критически переоценивая вывод. В Узбекистане целесообразно разработать стандарт обслуживания для таких ситуаций (возможно, силами Центрального банка или Ассоциации банков). Без четкой процедуры право на обжалование может остаться декларацией.

Под неадекватностью подразумевается ситуация, когда модель ИИ дает существенно некорректные или устаревшие результаты [21], не соответствующие реальной платежеспособности клиентов. Причины могут быть разными: модель обучена на нерелевантных данных, условия экономики изменились (например, пандемия изменила корреляции, а скоринг не перенастроен), или модель используется за пределами ожидаемой области (например, зарубежный алгоритм применен к другой стране без адаптации). Последствия – рост ошибок второго рода (незаслуженно отказанных хороших заемщиков) или первого рода (одобрение плохих рисков). Для банка это чревато убытками, для клиентов – несправедливостью и потерей возможностей [22]. Правовые механизмы здесь включают как рыночные стимулы (банк сам не хочет ошибаться, иначе потеряет прибыль), так и нормативные требования надежности. В EU AI Act требование точности и постоянного мониторинга предназначено для обеспечения адекватности моделей. В узбекской практике пока нет специальных норм, требующих от банков проверять качество своих ИИ-моделей, но этот выводится из общей обязанности банков управлять рисками (нормы регулятора по управлению кредитным риском). Хорошим решением было бы обязать банки при внедрении ИИ-скоринга проводить его валидацию – например, испытательный период, когда решения ИИ сверяются с решениями традиционной скоринговой системы или с экспертными оценками. Если выявляются значимые расхождения, модель дорабатывается. Стандарт ISO 23894 рекомендует именно такой итеративный подход к тестированию и улучшению ИИ-моделей. Также стоит требовать регулярного обновления модели: мир меняется, и вес факторов в скоринге должен пересматриваться (как отмечалось в исследовании OpenSCHUFA, использование старых версий алгоритма приводило к необоснованному занижению рейтингов).

Законодательно можно ввести норму о том, что провайдеры кредитного скоринга (включая внешние бюро) обязаны ежегодно ревизовать методики с учетом актуальных данных и научно-технического прогресса. Еще одна грань – киберриски и манипулирование алгоритмом: если злоумышленник узнает принципы скоринга, он может «оптимизировать» поведение для получения высокого балла, не будучи добросовестным заемщиком. Поэтому алгоритм должен быть устойчив к таким попыткам (например, не придавать чрезмерный вес легко инсценируемым факторам). Этот вопрос тоже стоит включить в повестку регулятора: контролировать, чтобы использование ИИ не порождало новых возможностей для мошенничества. Наконец, должна существовать обратная связь: если клиенту отказали, а потом выяснилось, что он надежный (например, предоставил дополнительные гарантии или другой банк его профинансировал, и он успешно вернул долг), то система должна учиться на таких ошибках. Юридически это не прописано, но бизнес-логика подсказывает внедрение подобных механизмов самообучения. В комплексе, обеспечение адекватности – это зона ответственности как создателей ИИ (их профессионализм), так и регуляторов (их внимательного надзора за результатами применения новых технологий). Узбекистану, нацелившемуся стать одним из центров ИИ в регионе, важно не только поощрять креативность разработчиков, но и требовать от них должного уровня качества решений, особенно затрагивающих финансы граждан.

Подводя итог обсуждению, отметим: международный опыт демонстрирует, что эффективное правовое управление рисками ИИ-скоринга требует комплексного подхода [23]. Изолированные меры (только запреты или только требования качества) не дадут результата, если не подкреплены другими. Например, запрет дискриминации нужно сочетать с прозрачностью, иначе её не обнаружить; а требование объяснимости бесполезно без права на оспаривание и механизма исправления решения. В ЕС формируется такой комплекс через сочетание GDPR (права субъекта), AI Act (требования к разработчикам и пользователям) и отраслевых норм (финансовое регулирование, антидискриминационные законы). В Узбекистане предстоит выстроить свою систему, учитывая национальные реалии – относительно невысокую цифровую грамотность населения, малое число местных разработчиков ИИ, но с другой стороны – большую роль государства в инициировании инноваций. При правильном подходе Узбекистан может избежать многих ошибок, допущенных на Западе, и сразу встроить принципы этичного и ответственного ИИ в развивающуюся экосистему финтех.

ЗАКЛЮЧЕНИЕ.

В ходе исследования установлено, что внедрение искусственного интеллекта в систему банковского скоринга сопряжено с четырьмя основными группами рисков: дискриминация**,** непрозрачность**,** нарушение прав потребителей **и** неадекватность алгоритмов. Сравнительный анализ показал, что на международном уровне сформировались правовые механизмы для управления каждым из этих рисков, хотя они еще находятся в процессе совершенствования. Европейский опыт (GDPR, проект AI Act, практика

судебных решений) демонстрирует стремление обеспечить баланс между инновациями и защитой граждан: вводятся гарантии против необоснованных автоматизированных решений, требования к качеству и прозрачности ИИ, процедуры надзора и ответственности разработчиков. Национальное законодательство Узбекистана в настоящее время предоставляет лишь общую основу (в виде прав в сфере персональных данных), но планируемые реформы и стратегия развития ИИ свидетельствуют о намерении внедрить более специализированное регулирование, основанное на лучших мировых практиках.

Adabiyotlar/Литература/References:

1. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260.
2. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89, 1-33.
3. Hanson, M., Cook, S., & Vaidhyanathan, S. (2019). The Apple Card Didn't 'See' Gender—and That's the Problem. Wired.
4. Bode, M., & Helberger, N. (2020). The GDPR and algorithmic decision-making – Safeguarding individual rights but forgetting society. Journal of Consumer Policy, 43, 525-542.
5. Kearns, M., & Roth, A. (2019). The ethical algorithm: The science of socially aware algorithm design. Oxford University Press.
6. Kaminski, M. E., & Malgieri, G. (2021). Multi-layered explanations from algorithmic impact assessments in the GDPR. In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency.
7. Felländer, A., Siri, S., & Teigland, R. (2018). The three phases of regulatory development for AI: A proposed model for balancing innovation and risk. Scandinavian Journal of Risk and Insurance, 34(2), 76-95.
8. Zweigert, K., & Kötz, H. (1998). Introduction to comparative law. Oxford University Press.
9. Article 29 Working Party. (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.
10. Malgieri, G. (2023). The CJEU's SCHUFA Decision: Automated Credit Scoring Under Art. 22 GDPR. European Data Protection Law Review, 9(3), 386-395.
11. Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International, 22(4), 97-112.
12. Dignum, V. (2023). A comprehensive approach to AI risk management. Nature Machine Intelligence, 5, 706-714.
13. Бегматов, А. С. (2020). Правовые аспекты защиты персональных данных в Республике Узбекистан. Вестник ТГЮУ, 4, 56-67.
14. Министерство цифровых технологий Республики Узбекистан. Стратегия развития искусственного интеллекта URL: https://gov.uz/ru/digital/pages/about
15. Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., & Walther, A. (2022). Predictably unequal? The effects of machine learning on credit markets. The Journal of Finance, 77(1), 5-47.
16. Zednik, C. (2021). Solving the black box problem: A normative framework for explainable artificial intelligence. Philosophy & Technology, 34, 265-288.
17. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 16, 18.
18. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence

(XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115.
19. Federal Trade Commission. (2018). Fair Credit Reporting Act provisions and requirements relating to consumer notifications.
20. Ramsay, I. (2016). Consumer law and policy: Text and materials on regulating consumer markets. Bloomsbury Publishing.
21. Hand, D. J., & Henley, W. E. (1997). Statistical classification methods in consumer credit scoring: a review. Journal of the Royal Statistical Society: Series A (Statistics in Society), 160(3), 523-541.
22. Thomas, L. C. (2009). Consumer credit models: Pricing, profit and portfolios. Oxford University Press, 228-236.
23. Waldman, A. E. (2020). Power, process, and automated decision-making. Fordham Law Review, 88(2), 613-648.