

Применение технологии искусственного интеллекта

В Банке действует Политика применения технологии искусственного интеллекта (далее – Политика), одобренная Правлением Банка и утвержденная Советом директоров Банка. Политика определяет цели, задачи и принципы применения технологии искусственного интеллекта (далее – ИИ) в процессах оказания банковских услуг, а также порядок внедрения, использования и контроля систем ИИ в деятельности Банка.

Политика разработана в соответствии с требованиями законодательства Республики Казахстан, включая Закон РК «О банках и банковской деятельности в Республике Казахстан», Закон РК «О персональных данных и их защите», Закон РК «Об информатизации», нормативные акты Агентства РК по регулированию и развитию финансового рынка, нормативные акты Агентства РК по регулированию и развитию финансового рынка, а также основывается на NIST Artificial Intelligence Risk Management Framework и Регламенте ЕС «AI Act».

Политика обязательна к соблюдению всеми работниками Банка, а также третьими лицами при планировании и осуществлении деятельности, связанной с применением технологии ИИ, включая разработку, внедрение, эксплуатацию и контроль систем ИИ.

1. Основные принципы применения ИИ

Применение ИИ в Банке основывается на следующих принципах:

Законность – строгое соблюдение этических и моральных норм при проектировании, разработке, использовании и развитии ИИ с соблюдением законодательных актов РК;

Прозрачность – доступность понимания алгоритмов принятия решений ИИ и объяснимость определяющих факторов в ходе данного процесса;

Справедливость – обеспечение равенства и признания достоинства каждого человека, его равной ценности и прав, исключая любую дискриминацию;

Надежность – использование отказоустойчивых вычислительных и инфраструктурных решений, при этом разработчики и собственники технологий и систем ИИ гарантируют их функционирование только в заявленных целях, исключая использование скрытых алгоритмов и незадекларированных возможностей;

Обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных объектов информатизации ИИ Банка;

Обеспечение конфиденциальности – соблюдение требований законодательства РК при сборе, обработке, хранении данных при использовании ИИ, гарантирующее соответствующую защищенность данных (включая защиту от несанкционированного доступа или незаконной обработки/передачи/распространения/хранения);

Кибер-устойчивость – защищенность от внешних и внутренних угроз, включая фальсификацию данных, вмешательство и манипуляции;

Риск-ориентированность – определение потенциальных рисков, связанных с применением ИИ в бизнес-процессах, и внедрение политики управления данными рисками;

Контролируемость – обеспечение активного человеческого участия в контроле и управлении процессом принятия решений, постоянный мониторинг и критическая оценка функционирования систем ИИ.

Перечисленные принципы реализуются с учетом Регламента ЕС «AI Act», на котором основывается Политика: функционирование систем ИИ гарантируется только в заявленных целях, исключая скрытые алгоритмы, незадекларированные возможности и любую дискриминацию, в том числе практики, относимые Регламентом ЕС «AI Act» к запрещенным, – манипулятивное воздействие, эксплуатацию уязвимостей человека, социальный скоринг и несанкционированное биометрическое наблюдение.

2. Права клиентов

Банк обеспечивает реализацию следующих прав клиентов:

Право знать. Клиент имеет право знать, участвует ли ИИ в принятии решений, касающихся его финансовых активов в Банке, в соответствии с законодательством РК;

Право обжалования. Все решения, принятые с участием ИИ, могут быть обжалованы через установленную процедуру, включая этап привлечения к процедуре работника Банка и/или представителей разработчиков/поставщиков системы ИИ (в случае если система ИИ была разработана сторонними/третьими лицами для Банка);

Право на отказ. Клиент вправе отказаться от участия в автоматизированных процессах, если это не противоречит законодательству РК, в том числе право отзыва разрешения на сбор и обработку данных;

Право на информацию о применении ИИ. По запросу клиента Банк обязуется предоставлять необходимую информацию о применении ИИ при обработке его данных, в рамках законодательства РК;

Право на обеспечение непередачи личных данных третьим лицам. Банк не предоставляет данные о клиентах, включая обезличенные, третьим лицам, общим пространствам данных и т.п., если такое предоставление не является требованием законодательства РК.

3. Внутренняя оценка рисков

Перед внедрением каждая система ИИ подлежит внутренней оценке рисков по следующим критериям: влияние на клиента или контрагента, работника, бизнес-процессы и репутацию Банка; обработка/хранение персональных и чувствительных данных и защищаемой информации Банка; соблюдение требований по защите персональных данных и защищаемой информации, в случае если система ИИ разработана сторонним/третьим лицом для Банка, в том числе требований по трансграничной передаче персональных данных клиента; соблюдение требований информационной безопасности, принятых Банком согласно законодательству РК и стандартам информационной безопасности Банка; автономность принятия решений; возможность дискриминации; качество данных; неотказуемость действий; обратимость решений работниками Банка.

Оценка рисков оформляется в виде карты рисков: каждый риск описывается (потенциальные места возникновения, источники риска, события, ведущие к риску) и оценивается (финансовые и нефинансовые последствия), по каждому риску прорабатываются

мероприятия по его снижению. Обязательному включению в карту подлежат этические, технические, операционные и регуляторные риски. Защита от рисков реализуется путем соблюдения трех линий защиты согласно нормативным актам АРРФР и ВНД Банка в области управления рисками.

4. Жизненный цикл систем ИИ

Банк реализует управление полным жизненным циклом системы ИИ, включая рассмотрение, проектирование, разработку или внедрение, тестирование, ввод в эксплуатацию, эксплуатацию, сопровождение, мониторинг и постоянную оценку эффективности (включая непрерывный процесс улучшения системы ИИ), а также вывод из эксплуатации. Для каждой системы ИИ определяются ее Бизнес-владелец, Владелец данных, оператор и ИТ-менеджер (администратор) из числа работников Банка, а также информационные активы, вовлеченные в систему ИИ и/или необходимые для ее поддержания.

5. Управление и контроль

Управление процессом применения ИИ возлагается на коллегиальный орган – Комитет по ИИ, уполномоченный принимать решения по задачам применения систем ИИ и обеспечивающий централизацию управления ИИ и следование принципам применения ИИ. В состав Комитета по ИИ в обязательном, но не ограниченном порядке включаются представители подразделений по управлению рисками, информационным технологиям, информационной безопасности и управлению данными Банка. Комитет по ИИ определяет целевые сферы применения ИИ. Любая исследовательская работа в сфере ИИ в Банке ведется с обязательным уведомлением Комитета по ИИ.

Банк разрабатывает и реализует внутренние процедуры, регламентирующие процессы применения ИИ, включая формирование и ведение перечня используемых систем ИИ, предоставление ежегодной отчетности по рисковому профилю ИИ, регламент разработки и применения ИИ, типовую карту рисков и способы управления ими, а также порядок определения целевых сфер применения ИИ.

6. Мониторинг и отчетность

С целью оценки деятельности и достигнутого прогресса Банка в части реализации принципов Политики осуществляются контроль и мониторинг реализации ИИ-проектов, соответствия деятельности Банка в сфере ИИ положениям Политики и законодательству РК. Комитет по ИИ определяет перечень, формат и периодичность предоставления отчетности Совету директоров Банка. Владельцем и ответственным за реализацию Политики является подразделение Банка, ответственное за управление данными и ИИ. Работники Банка, включая должностных лиц, несут ответственность за неисполнение и (или) ненадлежащее исполнение положений Политики.