УДК 001.5

Казакова Мария Сергеевна, кандидат технических наук, доцент, Поволжский государственный университет телекоммуникаций и информатики, г. Самара
Крюкова Галина Александровна, магистрант, Поволжский государственный университет телекоммуникаций и информатики, г. Самара

ОГРАНИЧЕНИЯ И РИСКИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СППР ГОССЕКТОРА

Аннотация

В данной статье рассматриваются ограничения и риски применения технологий искусственного интеллекта при внедрении систем поддержки принятия решений в предприятия госсектора.

Рассматривается роль ИИ в архитектуре СППР, а также особенности его использования в госсекторе. Основное внимание уделено систематизации рисков, возникающих при внедрении ИИ, включая технические, правовые, этические и операционные аспекты, а также их влиянию на надежность, прозрачность и легитимность решений.

Отдельный раздел посвящён международным и прикладным методикам оценки рисков и воздействия ИИ в СППР, включая AIA, ALTAI и DPIA, а также положениям Европейского регламента об искусственном интеллекте (AI Act). Дополнительно рассматриваются требования к обработке, защите и обезличиванию данных, используемых в ИИ-системах госсектора. Результаты исследования могут быть использованы при разработке и эксплуатации СППР для повышения управляемости рисков и обеспечения соответствия правовым и этическим нормам.

Annotation

This article examines the limitations and risks of using artificial intelligence technologies in implementing decision support systems in public sector enterprises.

The article examines the role of AI in decision support system architecture and the specifics of its use in the public sector. It focuses on systematizing the risks arising from AI implementation, including technical, legal, ethical, and operational aspects, as well as their impact on the reliability, transparency, and legitimacy of decisions.

A separate section is devoted to international and applied methodologies for assessing the risks and impact of AI in decision support systems, including AIA, ALTAI, and DPIA, as well as the provisions of the European Artificial Intelligence Act. Requirements for the processing, protection, and anonymization of data used in AI systems in the public sector are also discussed. The results of this study can be used in the development and operation of decision support systems to improve risk management and ensure compliance with legal and ethical standards.

Ключевые слова: СЭД, ИИ, СППР, госсектор,, ограничения ИИ.

Keywords: EDMS, AI, decision support system, public sector, AI limitations.

Цифровая трансформация предприятий госсектора сегодня набирает обороты. Внедрение искусственного интеллекта позиционируется как ключевой инструмент для повышения эффективности, объективности и скорости принятия решений.

Стоит учитывать, что применение ИИ в системах поддержки принятия решений несет за собой уникальные риски. Их наличие делает данное исследование чрезвычайно актуальным.

Решения, которые принимаются в государственных учреждениях, напрямую влияют на права, благополучие, а также судьбы граждан страны. Человеческий фактор и предвзятость имеют большие последствия.

Актуальность данного исследования определяется необходимостью не слепого внедрения искусственного интеллекта в предприятия госсектора,

а критического анализа и учета рисков для применения превентивных мер, обеспечивающих безопасное и законное использование технологии.

Целью данного исследования является выявить и проанализировать ключевые ограничения и риски внедрения ИИ в системы поддержки принятия решений госсектора.

Задачами являются:

- Классифицировать основные типы ограничений и рисков;
- Оценить существующую национальную стратегию;
- Описать методики оценки рисков для СППР.

Объект исследования – процесс принятия решений в госсекторе с использованием современных технологий.

Предмет исследования – совокупность ограничений, рисков и негативных социальных последствий, которые возникают при внедрении ИИ в СППР.

Система поддержки принятия решений – это компьютерные информационные системы, разработанные таким образом, чтобы помочь пользователям выбрать одно из множества альтернативных решений проблемы. Система является интерактивной и содержит организованный набор моделей, процедур, программного обеспечения и баз данных, что помогает лицам, принимающим решения, решать различные бизнес-проблемы.

В отличие от систем автоматического принятия решений, СППР не заменяет человека, а помогает ему принимать решения, усиливая когнитивные способности, предоставляя инструменты для анализа данных, моделирования последствий принятого решения и оценки альтернативных исходов.

Компонентами классической СППР являются:

- Система управления данными. Здесь происходит сбор и хранение релевантной информации.

– Система управления моделями содержит набор аналитических и математических моделей. К таким относятся оптимизационные, имитационные и прогнозные модели.

Пользовательский интерфейс, как инструмент для формулировки запросов и взаимодействия пользователя с системой.

Что же касается роли ИИ в системах, то его ключевой ролью является в усилении качества и обоснованности принимаемых решений человеком. стоит учитывать следующую, возможно ключевую характеристику СППР с ИИ. Это степень ее автономности. В зависимости от ее уровня, система может выступать как в роли советника или, как было сказано выше, партнера, так и полностью автономного субъекта принятия решений.

Ниже приведена градация по влиянию искусственного интеллекта на итоговое решение:

1. Информационно-справочные системы, где ИИ визуализирует данные и решение остается за человеком.
2. Рекомендательные системы-консультанты. ИИ предлагает несколько вариантов решений с оценкой рисков и обоснованием. Сотрудник проводит анализ альтернативных решений и самостоятельно принимает окончательное.
3. Системы-партнеры представляют собой коллаборацию человека и ИИ, где последние в совместном режиме исследуют проблемную область и формируют решение.
4. Автономные системы. ИИ принимает решения, но по строго установленным критериям в узких областях, где необходима быстрая реакция и человек не способен с ней справиться. В предприятиях госсектора такие системы неприменимы в связи с ограниченностью и этической проблематикой.

Несомненно, внедрение ИИ в госсектор формирует комплекс взаимосвязанных рисков. Их можно распределить на четыре категории: технические, правовые, этические и операционные. Для того, чтобы принять

решение о внедрении ИИ в свое предприятие необходимо понимать причину и последствия этих рисков.

Группа технических рисков связаны с ограничениями и сбоями в самой технологии, ее алгоритмах и данных, хранящихся в ней.

Наиболее важным и критичным риском является необъективность. Алгоритмы искусственного интеллекта обучаются на исторических данных, которые в свою очередь могут содержать скрытые предубеждения или замысел. При наличие таковых, ИИ может не только воспроизвести, но и усилить эти паттерны, что приведен к системным нарушениям.

Следующим рисков является так называемый «эффект черного ящика». Объясняется это тем, что сложные модели не могут предоставить человеку понятное для него объяснение сформированного решения. В госсекторе такой риск является критическим, что не позволяет системе быть полностью автономной или принимать серьезные решения самостоятельно.

Некоторые модели ИИ чувствительны к наборам данных, что может привести к ошибкам при наличии измененных вводных параметров.

В ситуациях принятого неверного решения, которое повлекло за собой вред или дорогостоящую ошибку, встает вопрос – а кто несет ответственность за такой исход.

Стоит учитывать также, что решения в государственных учреждениях должны основываться на четких нормах. Решения, принимаемые «черным ящиком», не поддаются традиционной правовой проверке на соответствие закону, что ставит под сомнение сам принцип верховенства права.

Интенсивное использование ИИ, особенно для профилирования, прогнозной аналитики и отслеживания, может нарушать принципы минимизации данных, целевого использования и права н приватность.

Передача значительной части аналитики и принятия решений алгоритмам может привести к «автоматизации предвзятости» и снижению критического мышления у сотрудников. Таким образом формируется

«эффект слепого доверия». Человек верит и просто идет дальше по интерфейсу системы, не вникая в суть задачи.

Процессы разработки и внедрения ИИ в госсекторе часто непрозрачны для общества. Граждане, на которых влияют эти системы, не имеют возможности участвовать в обсуждении их дизайна и целей.

К операционным рискам относится неготовность сотрудников обучаться и переобучаться в использовании нового программного обеспечения.

Разработка, внедрение, поддержка и постоянный аудит качественных ИИ-систем требуют значительных финансовых, временных и инфраструктурных ресурсов, что может быть неподъемно для многих ведомств и ведет к зависимости от вендоров.

Стремление внедрить «модную» технологию без четкого понимания решаемой проблемы. ИИ становится самоцелью, а не инструментом, что приводит к созданию бесполезных или вредных систем.

Формирование национальной политики в области искусственного интеллекта в России носит комплексный и ускоренный характер.

Регуляторный ландшафт складывается вокруг двух ключевых осей: стратегического видения и стимулирования развития (через концепции, «стратегии» и дорожные карты) и создания правовых основ для внедрения и использования (через федеральные законы и подзаконные акты).

Национальная стратегия развития искусственного интеллекта до 2030 года утверждена Указом Президента РФ № 490 от 10.10.2019, с актуализацией в 2021 году. Данный документ задет долгосрочные ориентиры и вот его основные положения:

Целью стратегии является обеспечение ускоренного развития ИИ в РФ, достижение и поддержание лидерских позиций в сфере ИИ. Основными принципами является приоритет человека, безопасность и защищенность, прозрачность и предсказуемость, а также обеспечение конкуренции.

Ключевыми направлениями для госсектора являются:

- Стимулирование использования ИИ в государственном управлении и предоставлении государственных услуг.
- Развитие цифровой инфраструктуры.
- Поддержка образования и научных исследований в области ИИ.

Исходя из этого, данный документ прямо указывает на госуправление как на одну из приоритетных сфер внедрения ИИ.

Внедрение искусственного интеллекта в государственные системы поддержки принятия решений требует протоколов для выявления и минимизации сопутствующих рисков. Поскольку в России пока отсутствует единая обязательная национальная методика, адаптация международных фреймворков становится практической необходимостью.

Суть данного подхода – это прямое регулирование, вводящее классификацию ИИ-систем по уровню риска: неприемлемый, высокий, ограниченный, минимальный.

Для систем высокого риска устанавливаются обязательные требования и процедура оценки соответствия до выхода на рынок или внедрения.

Ключевыми требованиями для систем высокого риска являются:

- Систему управления рисками – непрерывный цикл на всем жизненном цикле системы.
- Качество данных и документирование – использование непредвзятый наборов данных с соответствующей документацией.
- Прозрачность и информационное обеспечение пользователя, что подразумевает предоставление ясных руководств для пользователей о назначении и ограничениях системы.
- Надежность, точность и кибербезопасность. Необходима техническая устойчивость к внешним атакам и ошибкам.

Обычно проводится внутренняя оценка соответствия с последующим составлением технической документации, декларации соответствия и регистрацией системы в единой европейской базе данных.

Для России схож разрабатываемый российский закон «Об ИИ», который заявляет о схожем риск-ориентированном подходе. Так, структура требования AI Act может стать основной для будущих национальных стандартов оценки СППР.

Подход ALTAI разработан Европейской комиссией. Этот инструмент позволяет организациям проверить ИИ-систему на соответствие 7 ключевым требованиям:

1. Человеческий надзор и контроль
2. Техническая надежность и безопасность
3. Конфиденциальность и управление данными
4. Прозрачность
5. Многообразие, недискриминационность и справедливость
6. Социальное и экологическое благополучие
7. Подотчетность

Этот инструмент реализован в виде онлайн-опросника, который выявляет пробелы и предлагает рекомендации.

Данный подход применим для систем в России, поскольку имеет низкий порог внедрения и не требует изменений в законодательстве. Он охватывает не только технические, но и этические, социальные аспекты.

Подход DPIA направлен на выявление и минимизацию рисков для прав и свобод физических лиц, которые возникают при обработке персональных данных. Профилирование и автоматизированное принятие решений – прямые триггеры для проведения DPIA.

Ниже представлены ключевые этапы подхода DPIA:

1. Описание обработки и ее целей.
2. Оценка необходимости и соразмерности обработки.

3. Идентификация рисков для прав субъектов данных (дискриминация, финансовые потери, ущемление прав).
4. Определение мер по смягчению рисков.
5. Документирование и интеграция результатов в проект.

Ст. 36.1 Федерального закона 152-ФЗ вводит понятие «Оценка воздействия обработки персональных данных на защищенность персональных данных». Это является прямым аналогом DPIA. Проведение оценки обязательно при использовании новых технологий автоматизированной обработки.

Любая СППР с ИИ, обрабатывающая персональные данные, подпадает под требование проведения такой оценки по 152-ФЗ.

В условиях цифровой трансформации и роста объемов данных СППР активно интегрируются с элементами искусственного интеллекта. Это сочетание позволяет не только проводить анализ сложных ситуаций, а также упрощает функциональные возможности СППР.

В ходе данной статьи было проведено комплексное рассмотрение вопросов применения искусственного интеллекта в системах поддержки принятия решений.

В первой части были проанализированы сущность СППР и место ИИ в их архитектуре, что позволило определить роль интеллектуальных методов в повышении эффективности и обоснованности управленческих решений.

Рассмотрены технические, правовые, этические и операционные риски, а также показано их влияние на надёжность, безопасность и допустимость применения интеллектуальных систем в различных сферах деятельности.

Сформулированы требования к обработке и обезличиванию данных при использовании ИИ, что подчеркнуло ключевую роль защиты персональной и чувствительной информации в процессе разработки и эксплуатации ИИ-ориентированных СППР.

Проведённый анализ позволяет сделать вывод о необходимости интеграции технических, правовых и этических механизмов управления рисками для обеспечения устойчивого и ответственного применения искусственного интеллекта в системах поддержки принятия решений.

1. Практика применения искусственного интеллекта в государственном управлении: возможности и риски (Республика Башкортостан) // Научная сеть. – 2024. – URL: https://scinetwork.ru/articles/6064 (дата обращения: 20.04.2026).

2. Шпакова Р. Н., Городецкий Д. И. Перспективы использования технологий искусственного интеллекта в региональном стратегическом планировании // Региональная экономика и управление. – 2025. – № 1. – С. 45–53.

3. Кабанова Е. Е. Искусственный интеллект в государственном управлении: ключевые проблемы и перспективы применения // Russian Journal of Management. – 2025. – Т. 13, № 2. – URL: https://asu.infra-m.ru/ru/nauka/article/95536/view (дата обращения: 20.04.2026).

4. Кузнеченко И. М. Риски организации и реализации процесса принятия решений на основании аналитики больших данных и искусственного интеллекта // Государственное управление. Электронный вестник. – 2024. – № 104.

5. Обзор российских систем электронного документооборота [Электронный ресурс] // Библиотека информационной безопасности. — Режим доступа: https://lib.itsec.ru/articles2/focus/obzor_ros_sed (дата обращения: 20.04.2026).

6. Загайнов М. Р. Политико-правовой опыт России в отношении применения искусственного интеллекта во внутренней и внешней политике // Социально-политические науки. – 2025. – Т. 15, № 1. – С. 110–118. – URL: https://journals.rcsi.science/2223-0092/article/view/313361 (дата обращения: 21.04.2026).

Информация о себе:
Крюкова Г.А. gp1201@yandex.ru