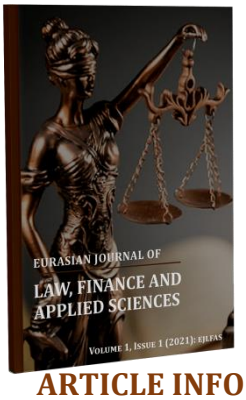
EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
IF = 7.984 www.in-academy.uz



THE IMPACT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS ON THE STORAGE OF CONFIDENTIAL INFORMATION IN THE REPUBLIC OF UZBEKISTAN

Shukhratjon Yokubov
Lecturer of the Department of Intellectual Property Law
Tashkent State Law University
E-mail: shukhrat.y2000@gmail.com
https://doi.org/10.5281/zenodo.14709608

ARTICLE INFO

Received: 15th January 2025
Accepted: 20th January 2025
Online: 21th January 2025

KEYWORDS

Artificial intelligence, personal data, confidentiality, data protection, risks of AI systems, adaptation of legislation, rights of data subjects.

ABSTRACT

The article analyzes the impact of artificial intelligence (AI) technology development on the practice of storing and protecting personal data of citizens in the context of Uzbekistan's legal framework. The author examines the Law "On Personal Data" as the basic document regulating the collection, storage, and use of confidential information. It is noted that the implementation of AI systems opens new opportunities for improving data protection mechanisms, but at the same time carries potential risks of leaks and misuse. The article provides recommendations for adapting the regulatory framework to new realities, including introducing requirements for transparency and accountability of AI algorithms, strengthening the rights of data subjects, and implementing risk assessment mechanisms. The article emphasizes the need for a comprehensive approach involving government, business, and society to ensure a balance between technological development and privacy protection.

ВЛИЯНИЕ РАЗВИТИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Шухратжон Ёкубов
Преподаватель кафедры права интеллектуальной собственности
Ташкентского государственного юридического университета
E-mail: shukhrat.y2000@gmail.com
https://doi.org/10.5281/zenodo.14709608

ARTICLE INFO

Received: 15th January 2025
Accepted: 20th January 2025
Online: 21th January 2025

KEYWORDS

Искусственный интеллект, персональные данные,

ABSTRACT

Статья посвящена анализу влияния развития технологий искусственного интеллекта (ИИ) на практику хранения и защиты персональных данных граждан в контексте правового поля Узбекистана. Автор рассматривает Закон «О персональных данных» как базовый документ, регламентирующий

конфиденциальность, защита информации, риски ИИ-систем, адаптация законодательства, права субъектов данных.

сбор, хранение и использование конфиденциальной информации. Отмечается, что внедрение ИИ-систем открывает новые возможности для совершенствования механизмов защиты данных, но в то же время несет потенциальные риски утечек и недобросовестного использования. В статье даются рекомендации по адаптации нормативно-правовой базы к новым реалиям, включающие введение требований к прозрачности и подконтрольности ИИ-алгоритмов, усиление прав субъектов данных, внедрение механизмов оценки рисков. Подчеркивается необходимость комплексного подхода, вовлекающего государство, бизнес и общество для обеспечения баланса между технологическим развитием и защитой неприкосновенности частной жизни.

Развитие технологий искусственного интеллекта (ИИ) оказывает значительное влияние на различные сферы жизни общества, в том числе на вопросы хранения и защиты конфиденциальной информации, особенно персональных данных граждан. В Республике Узбекистан принят ряд законодательных актов, регулирующих правоотношения в этой области, ключевым из которых является Закон «О персональных данных» от 2 июля 2019 года № ЗРУ-547.

В данной работе анализируется влияние развития систем ИИ на практику хранения конфиденциальной информации в контексте правового поля Узбекистана, очерченного упомянутым Законом. Рассматриваются как возможности, которые предоставляют интеллектуальные системы для совершенствования механизмов защиты данных, так и потенциальные риски и вызовы, связанные с их применением. На основе проведенного анализа предлагаются рекомендации по адаптации регуляторных подходов и практик хранения конфиденциальной информации к новым технологическим реалиям.

Закон «О персональных данных» как базовый документ в сфере защиты конфиденциальной информации

Закон «О персональных данных», вступивший в силу в октябре 2019 года, стал первым в Узбекистане комплексным нормативно-правовым актом, регламентирующим общественные отношения, связанные со сбором, систематизацией, хранением, изменением, дополнением, использованием, предоставлением, распространением, передачей, обезличиванием и уничтожением персональных данных (ст. 4). Его принятие ознаменовало формирование базовой правовой основы для защиты конфиденциальной информации о гражданах в условиях цифровой трансформации и развития систем ИИ.

Закон определяет персональные данные как зафиксированную на электронном, бумажном и (или) ином материальном носителе информацию, относящуюся к определенному физическому лицу или дающую возможность его идентификации (ст.

4). Таким образом, в сферу его действия подпадает широкий спектр сведений о гражданах, которые собираются, хранятся и обрабатываются как государственными органами, так и коммерческими и некоммерческими организациями.

Документ устанавливает ключевые принципы обработки персональных данных, к числу которых относятся: законность целей и способов обработки, точность и достоверность сведений, их конфиденциальность и защищенность, равенство прав участников соответствующих правоотношений (ст. 5). Особое внимание уделяется вопросам согласия субъекта на обработку его персональных данных, уведомления об осуществляемых с ними действиях, ограничения доступа третьих лиц к конфиденциальной информации.

Закон вводит институт уполномоченного государственного органа в области персональных данных (Государственный центр персонализации при Кабинете Министров), который наделяется широким кругом контрольных и надзорных полномочий (ст. 8). В числе его основных функций – ведение Государственного реестра баз персональных данных, утверждение требований и методических рекомендаций по их защите, рассмотрение обращений граждан, связанных с обработкой их персональной информации.

Значительный блок норм Закона посвящен правам субъектов персональных данных (граждан) и корреспондирующим им обязанностям операторов (лиц, организующих и осуществляющих обработку). Ключевые права граждан включают получение информации о наличии и составе собираемых персональных данных, доступ к ним, возможность требовать их уточнения или уничтожения, обжалование неправомерных действий операторов (ст. 30). Операторы, в свою очередь, должны обеспечивать конфиденциальность и безопасность обрабатываемых сведений, реагировать на запросы граждан, уведомлять их о предпринимаемых действиях, согласовывать передачу информации третьим лицам (ст. 31).

Отдельные статьи Закона регламентируют особенности обработки специальных категорий персональных данных (раскрывающих расовое или национальное происхождение, политические и религиозные взгляды, состояние здоровья и т.п.), а также биометрических и генетических сведений. Устанавливаются более строгие требования в части получения согласия субъекта на их сбор и использование, допускается обработка таких данных без согласия только в прямо предусмотренных законом случаях (ст. 25-26).

Наконец, Закон закрепляет гарантии защиты персональных данных, обязывая операторов принимать правовые, организационные и технические меры по обеспечению их конфиденциальности и безопасности (ст. 27). Устанавливается ответственность лиц, виновных в нарушении требований законодательства в этой сфере (ст. 33).

Таким образом, Закон «О персональных данных» формирует комплексную систему регулирования сбора, хранения и использования конфиденциальной информации о гражданах. Он содержит ряд важных норм и механизмов, направленных как на защиту прав субъектов персональных данных, так и на установление четких рамок и процедур для организаций, выступающих в роли операторов. Вместе с тем,

документ лишь в самом общем виде затрагивает вопросы применения технологий ИИ в процессе обработки персональных данных, что требует дальнейшего нормативного уточнения с учетом динамичного развития этой сферы.

Развитие технологий ИИ и регулирование их применения в Узбекистане

Узбекистан в последние годы предпринимает активные шаги по развитию и внедрению технологий искусственного интеллекта в различных отраслях экономики и государственного управления. Утверждена Национальная стратегия по развитию искусственного интеллекта до 2030 года, которая предусматривает меры по созданию необходимой инфраструктуры, подготовке кадров, стимулированию исследований и разработок в этой сфере.

Ключевыми направлениями применения ИИ определены здравоохранение (ранняя диагностика заболеваний, персонализированная медицина, разработка новых лекарств), образование (адаптивное обучение, анализ образовательных данных), транспорт и логистика (беспилотные системы, оптимизация маршрутов), сельское хозяйство (точное земледелие, управление агропроцессами), промышленность (предиктивное обслуживание оборудования, контроль качества), государственное управление (автоматизация рутинных процессов, поддержка принятия решений, выявление рисков) и ряд других сфер.

Наряду с этим, внедрение технологий ИИ порождает ряд вопросов с точки зрения защиты конфиденциальной информации и персональных данных граждан. ИИ-системы способны собирать и анализировать огромные массивы данных из самых разных источников, что повышает риски утечки и недобросовестного использования чувствительной информации. Многие ИИ-алгоритмы работают по принципу «черного ящика», затрудняя интерпретацию и объяснение получаемых результатов. Это создает угрозу дискриминации и нарушения прав человека при принятии юридически значимых решений системами ИИ.

В связи с этим важной задачей становится адаптация нормативно-правовой базы к реалиям ИИ-эпохи и формирование механизмов контроля за оборотом данных в рамках соответствующих систем. В частности, эксперты указывают на необходимость:

- уточнения правового статуса ИИ-систем и распределения ответственности между их разработчиками, операторами и пользователями;
- установления требований к прозрачности, объяснимости и подотчетности ИИ-алгоритмов;
- определения условий и процедур использования ИИ для обработки персональных данных и принятия решений в отношении граждан;
- закрепления права человека на получение информации о применяемых к нему ИИ-системах и обжалование их выводов;
- введения дополнительных гарантий при обработке чувствительной информации (биометрических, генетических и медицинских данных) с помощью ИИ.

В Узбекистане постепенно формируются нормативные рамки для регулирования применения систем ИИ при работе с персональными данными и конфиденциальной информацией граждан. Вместе с тем, многие вопросы в этой сфере еще предстоит урегулировать на законодательном и подзаконном уровне, определив четкие критерии

и процедуры допустимого использования ИИ, права и обязанности участников соответствующих отношений, механизмы защиты интересов граждан.

Возможности систем ИИ для совершенствования защиты данных

Развитие технологий ИИ открывает новые возможности для совершенствования механизмов хранения и защиты конфиденциальной информации и персональных данных. Интеллектуальные системы способны автоматизировать и удешевить многие процессы по обеспечению безопасности данных, которые раньше требовали больших затрат ресурсов и времени. Рассмотрим основные направления применения ИИ в этой сфере.

Во-первых, ИИ может использоваться для выявления и прогнозирования угроз информационной безопасности. Интеллектуальные алгоритмы анализируют огромные массивы данных о киберинцидентах, выделяя общие паттерны и индикаторы компрометации. Это позволяет оперативно обнаруживать аномальную активность в корпоративных сетях и системах хранения данных, блокировать развитие атак на ранних стадиях. ИИ-модели способны выявлять скрытые уязвимости в IT-инфраструктуре, предсказывать возможные векторы и цели атак злоумышленников.

Примерами практического применения таких решений являются ИИ-системы выявления вторжений (AI-системы выявления вторжений (AI-powered Intrusion Detection Systems, AI-IDS), которые в режиме реального времени анализируют сетевой трафик и идентифицируют подозрительные события. Они используют методы машинного обучения для детектирования аномальных отклонений от типовых шаблонов активности пользователей и устройств. Это позволяет выявлять продвинутые угрозы, которые не определяются традиционными сигнатурными методами.

Другой пример - ИИ-платформы для предиктивной аналитики киберрисков. Они агрегируют данные об уязвимостях, угрозах и инцидентах безопасности из множества внутренних и внешних источников (системы мониторинга, сенсоры, открытые БД, даркнет и т.д.). Затем ИИ-модели анализируют эти данные, чтобы прогнозировать наиболее вероятные сценарии атак, оценивать потенциальный ущерб, определять приоритетные направления для усиления защиты.

Во-вторых, ИИ незаменим для анализа и классификации информации в целях обеспечения требуемого уровня конфиденциальности. В крупных организациях циркулируют огромные объемы неструктурированного контента (документы, письма, чаты и т.п.), в которых могут содержаться чувствительные персональные данные и коммерческие секреты. Традиционные методы категоризации контента на основе правил не справляются с этой задачей.

ИИ-системы позволяют автоматически классифицировать информационные активы по уровню конфиденциальности на основе анализа их содержания. Интеллектуальные модели обучаются выявлять признаки наличия защищаемых сведений (ФИО, адреса, номера документов, ключевые слова и т.п.) в неструктурированных данных. На основе этого каждому документу или фрагменту

присваивается метка конфиденциальности, в соответствии с которой ограничивается доступ и передача информации.

Пример такого решения - платформа Microsoft Information Protection. Она использует ИИ для автоматической маркировки документов и писем на основе анализа содержимого и контекста (отправитель, получатели, тема). ИИ-модели платформы постоянно дообучаются, повышая точность классификации. Платформа интегрируется с офисными приложениями, корпоративными порталами, облачными хранилищами, обеспечивая сквозную защиту конфиденциальной информации.

В-третьих, ИИ помогает автоматизировать процессы обеспечения приватности данных. Компании должны соблюдать требования законодательства и стандартов в части получения согласий субъектов, предоставления им доступа к собираемым сведениям, удаления данных по запросу и т.д. Ручная обработка таких запросов отнимает много времени и чревата ошибками.

ИИ-решения берут на себя управление цифровыми согласиями пользователей, автоматически проверяют их наличие при попытке обработки персональных данных. Чат-боты и виртуальные ассистенты на базе ИИ могут принимать и обрабатывать запросы граждан на предоставление информации и отзыв согласий, формируя необходимые данные из внутренних систем. ИИ-алгоритмы кластеризации и обезличивания данных помогают подготовить их для аналитического использования без угрозы деанонимизации.

Так, стартап OneTrust предлагает платформу автоматизации конфиденциальности на базе ИИ. Решение сканирует IT-системы компании, находит хранящиеся персональные данные и связывает их с цифровыми согласиями пользователей. Автоматические процессы обрабатывают запросы субъектов на доступ, исправление и удаление данных. Специальный ИИ-модуль в режиме реального времени оценивает риски при обработке данных и формирует рекомендации по их минимизации.

Риски и вызовы использования ИИ в сфере защиты данных

Наряду с открывающимися возможностями, применение систем ИИ для работы с конфиденциальной информацией и персональными данными несет ряд потенциальных рисков и вызовов. Они связаны как с текущими ограничениями технологий, так и с опасностью злонамеренного использования ИИ. Основные проблемные зоны включают:

1) Низкую интерпретируемость и прозрачность ИИ-моделей. Многие современные алгоритмы глубокого обучения работают по принципу «черного ящика». Они выдают результаты и рекомендации, но не объясняют в явном виде логику своих выводов. Это критично в таких чувствительных областях, как медицинская диагностика или выявление финансовых преступлений. Решения ИИ, принимаемые в отношении граждан, должны быть понятны и проверяемы.

Закрытость ИИ-моделей затрудняет аудит их работы на соответствие нормам законодательства о персональных данных. Непонятно, какие сведения система использует для обучения, как ограничивается их распространение, обеспечивается ли

право субъекта на удаление данных из обучающей выборки и т.д. Все это повышает риски незаметных утечек и нарушений конфиденциальности.

2) Трудности в обеспечении качества данных для обучения ИИ-моделей. Точность работы интеллектуальных алгоритмов напрямую зависит от объема и репрезентативности данных, на которых они обучаются и тестируются. При этом доступ к реальным конфиденциальным сведениям (медицинским записям, банковским транзакциям и т.п.) для тренировки ИИ, как правило, ограничен.

Использование для обучения синтетических или обезличенных данных не всегда обеспечивает необходимое качество моделей. Например, в 2021 г. стартап Recursion Pharma использовал генеративно-состязательные нейросети (GAN) для синтеза медицинских изображений в обход приватности. Однако сгенерированные снимки отличались от реальных, модели диагностики оказывались неточными. Риски для пациентов от использования таких ИИ-систем слишком велики.

3) Деанонимизацию и утечки данных из обучающих выборок. Для тренировки ИИ-моделей на конфиденциальных массивах данные обычно обезличиваются - удаляются прямые идентификаторы субъектов (имена, адреса и т.п.). Однако есть риск, что обученная модель «запомнит» четкие примеры из выборки и раскроет их по запросу. Злоумышленники могут использовать эту уязвимость для целевой деанонимизации граждан.

Так, в 2020 г. исследователи смогли восстановить персональную информацию из обучающей выборки языковой модели GPT-2, атакуя ее специально сформированными запросами. Модель точно воспроизвела несколько реальных конфиденциальных текстов, содержавших ФИО, адреса и телефоны людей. Учитывая чувствительность данных для обучения ИИ-систем, вопрос предотвращения таких утечек стоит очень остро.

4) Использование ИИ злоумышленниками для атак и вредоносной деятельности. Киберпреступники тоже применяют технологии ИИ, чтобы сканировать уязвимости, подбирать пароли, автоматизировать фишинговые рассылки, обходить системы защиты. С помощью ИИ-алгоритмов они могут анализировать большие массивы украденных данных, выявлять по косвенным признакам наиболее ценную информацию (должности, уровень доходов, круг контактов и т.д.).

ИИ-модели социальной инженерии обучаются на сливах данных и на основе публичного цифрового следа людей точечно подбирать методы воздействия: выявлять уязвимости, подделывать голоса для телефонных атак, генерировать персонализированный фишинговый контент. Растет опасность использования ИИ для подделки личности (deepfakes) в мошеннических и преступных целях.

5) Необходимость обеспечения безопасности самих ИИ-моделей. По мере распространения интеллектуальных систем в критически важных отраслях - энергетике, транспорте, здравоохранении, финансах - они сами становятся привлекательными целями для злоумышленников. Взлом или подмена моделей, определяющих уровень конфиденциальности данных, может привести к масштабным утечкам и нарушениям прав граждан.

Особую опасность представляют атаки на ИИ-модели по принципу «черного ящика», когда преступнику не нужно знать внутреннее устройство системы. Манипулируя входными данными, он добивается нужной ему реакции. Например, в одном исследовании ученые смогли обмануть ИИ-классификатор рентгеновских снимков, добавив в изображения визуально незаметный шум. В 100% случаев модель ошибочно диагностировала рак легких у здоровых пациентов. Такие атаки могут использоваться для целенаправленных утечек медданных.

Отдельного внимания требует безопасность децентрализованного машинного обучения, которое набирает популярность для работы с конфиденциальной информацией (например, в медицинских федеративных сетях). При таком подходе ИИ-модели обучаются локально на нескольких узлах без передачи самих данных. Но злоумышленник может скомпрометировать один из узлов, подменив градиенты модели для «отравления» обучения. Требуются новые методы защиты таких распределенных систем.

Таким образом, наряду с перспективами, внедрение ИИ в практику хранения и обработки конфиденциальной информации сопряжено с комплексом сложных технических, правовых и этических вызовов. Их преодоление требует активного сотрудничества регуляторов, разработчиков, владельцев данных и независимых экспертов. Нужны гибкие правовые нормы, стимулирующие внедрение передовых ИИ-решений при обязательном соблюдении прав и интересов граждан. Важную роль должно играть развитие стандартов и методов обеспечения прозрачности, безопасности и контролируемости ИИ-систем в чувствительных областях.

Рекомендации по адаптации нормативной базы

Закон «О персональных данных», принятый в 2019 году, заложил правовую основу для защиты конфиденциальной информации граждан в Узбекистане. Однако стремительное развитие и внедрение технологий ИИ ставит новые вопросы, требующие законодательного регулирования. Для эффективной адаптации правового поля целесообразно реализовать следующие шаги:

1) Ввести в Закон определение ИИ-систем, установить общие требования к их разработке и использованию. Четко обозначить, что применение ИИ для обработки персональных данных допускается, но должно отвечать принципам законности, прозрачности и подконтрольности. Использование ИИ не снимает с операторов ответственности за обеспечение конфиденциальности и безопасности сведений.

2) Закрепить право граждан на получение информации об используемых в отношении них ИИ-моделях, их назначении и основных принципах работы. Обязать операторов предоставлять по запросу сведения о целях применения ИИ, составе обрабатываемых данных, мерах по защите конфиденциальности. Определить исключения, когда раскрытие может ограничиваться (гостайна, риски для безопасности и т.п.).

3) Установить особые условия для обработки биометрических и генетических данных граждан с помощью ИИ. В частности, ввести требование получения отдельного явного согласия субъекта на использование таких сведений для обучения ИИ-моделей.

Закрепить право граждан запрещать применение их биометрии и генетической информации в ИИ-системах без достаточных правовых оснований.

4) Ввести дополнительные гарантии прав граждан при автоматизированном принятии юридически значимых решений системами ИИ (например, в части представления кредитов, распределения социальной помощи и т.д.). Обязать использовать прозрачные и проверяемые модели, предоставлять гражданам детальные разъяснения, обеспечивать возможность оспаривания и компенсации возможного вреда.

5) Регламентировать требования к обеспечению качества и репрезентативности данных для обучения ИИ-моделей, работающих с конфиденциальной информацией. Обязать операторов принимать меры по выявлению и устранению возможных ошибок и искажений в обучающих выборках. Установить необходимость периодической проверки точности и актуальности моделей на тестовых данных.

6) Определить правила обезличивания персональных данных, используемых для разработки ИИ-решений. Закрепить требования по удалению прямых идентификаторов, агрегированию, внесению случайных возмущений в выборки для затруднения последующей деанонимизации. Предусмотреть ответственность за умышленное или неосторожное раскрытие персональных данных из обучающих массивов.

7) Предусмотреть обязательную оценку рисков внедрения ИИ-систем для конфиденциальности и приватности граждан до начала их эксплуатации. Установить перечень вопросов, которые должны быть проанализированы: цели и способы использования ИИ, категории обрабатываемых данных, методы защиты, риски утечек и несанкционированного доступа, воздействие на права субъектов и т.д.

8) Усилить правовые механизмы надзора и контроля за ИИ-системами со стороны уполномоченного органа. Расширить его полномочия по проведению проверок, экспертизы ИИ-моделей, работающих с персональными данными. Уточнить составы правонарушений и меры ответственности операторов за несоблюдение требований по безопасности и конфиденциальности при использовании ИИ.

9) Предусмотреть меры поддержки внедрения перспективных методов защиты конфиденциальности при обработке данных ИИ-системами. В частности, установить преференции по налогам и сборам для организаций, применяющих продвинутые Privacy Enhancing Technologies (гомоморфное шифрование, федеративное обучение, дифференциальную приватность и т.п.).

10) Гармонизировать национальное законодательство с международными нормами и стандартами в области защиты персональных данных при использовании ИИ (документы ОЭСР, Совета Европы и т.д.). Предусмотреть механизмы трансграничного сотрудничества компетентных органов по вопросам контроля за ИИ-системами и расследования инцидентов с персональными данными.

Перечисленные предложения призваны создать сбалансированные регуляторные условия, способствующие развитию ИИ в Узбекистане при обеспечении должной защиты прав и свобод граждан. Важно выстроить постоянный диалог между

законодателями, регуляторами, бизнесом и экспертным сообществом для поиска оптимальных правовых решений, отвечающих динамике технологического прогресса.

Организационные и технические меры совершенствования защиты данных

Помимо адаптации нормативной базы, эффективное обеспечение конфиденциальности информации в условиях распространения ИИ-систем требует принятия комплекса организационных и технических мер как на уровне уполномоченных госорганов, так и на уровне операторов персональных данных. Ключевые направления работы включают:

1) Развитие методологии и стандартов оценки рисков ИИ-систем для защиты персональных данных. Уполномоченному органу необходимо сформировать четкие критерии и метрики анализа угроз безопасности и конфиденциальности на всех этапах жизненного цикла интеллектуальных решений - от проектирования и обучения моделей до эксплуатации и вывода из употребления.

2) Внедрение эффективных процедур аудита и сертификации ИИ-систем на соответствие нормам законодательства о персональных данных. Регулятор должен обладать инструментами и компетенциями для проверки прозрачности, безопасности и подконтрольности алгоритмов. Целесообразно задействовать потенциал независимых отраслевых центров компетенций по ИИ для проведения экспертизы решений.

3) Разработка механизмов объяснения логики принятия решений ИИ-моделями, затрагивающих права и интересы граждан. Уполномоченный орган совместно с научным сообществом должны определить унифицированные способы интерпретации и документирования таких алгоритмов. Операторы ИИ-систем обязаны обеспечить возможность получения человекочитаемых объяснений по запросу регуляторов и субъектов данных.

4) Обязательное определение ответственных за обеспечение конфиденциальности при использовании ИИ-инструментов в организациях. В дополнение к структурным подразделениям по защите данных, рекомендуется ввести должности специалистов по этическим аспектам ИИ (AI ethics officers). В их задачи должны входить выявление и контроль рисков интеллектуальных систем, взаимодействие с регуляторами, реагирование на обращения граждан.

5) Совершенствование систем управления согласиями граждан на обработку их персональных данных в ИИ-решениях. Операторам следует обеспечить удобные интерфейсы для отзыва ранее данных разрешений и запрета на использование сведений в алгоритмах. При этом должны приниматься меры для минимизации негативного влияния на работоспособность сервисов и сохранности агрегированных моделей.

6) Псевдонимизация и анонимизация персональных данных, применяемых для обучения и тестирования ИИ-моделей. Необходимо минимизировать использование прямых идентификаторов граждан (ФИО, паспортных данных и т.п.) в машиночитаемых массивах. Следует шире задействовать методы формирования синтетических выборок, не позволяющих установить личности реальных субъектов данных.

7) Обеспечение криптографической защиты конфиденциальных данных на всех этапах их обработки ИИ-инструментами. Операторам нужно внедрять современные методы шифрования, позволяющие анализировать информацию без расшифровки (гомоморфное шифрование). Это особенно важно при передаче данных между участниками кросс-организационного обучения моделей, использовании внешних ИИ-сервисов.

8) Защита самих ИИ-моделей от атак и несанкционированных модификаций со стороны внешних и внутренних злоумышленников. Требуется обеспечить безопасность интерфейсов обучения и вывода алгоритмов, применять методы выявления состязательных примеров (adversarial examples). Должны быть предусмотрены процедуры реагирования на инциденты ИБ с ИИ-системами.

9) Развитие компетенций сотрудников организаций в области приватности при использовании ИИ. Следует организовать специальные учебные программы по конфиденциальности данных для команд-разработчиков ИИ-решений, администраторов безопасности, менеджеров продуктов. Эти знания позволят учитывать требования защиты персональной информации изначально, на этапе проектирования интеллектуальных систем (принцип Privacy by Design).

10) Повышение осведомленности и цифровой грамотности граждан в части особенностей сбора и обработки их данных системами ИИ. Необходимо на доступном языке разъяснять права субъектов в отношении автоматизированно принимаемых решений, способы реализации этих прав. Важно вовлекать представителей гражданского общества в обсуждение вопросов этичного применения ИИ для работы с персональной информацией.

Безусловно, перечисленные меры не являются исчерпывающими и будут трансформироваться по мере развития технологического ландшафта. Однако они закладывают организационно-техническую основу для обеспечения конфиденциальности в ИИ-системах в среднесрочной перспективе. Скоординированная работа регуляторов, бизнеса и общества по этим направлениям позволит реализовать потенциал интеллектуальных решений для повышения качества услуг и процессов при соблюдении фундаментальных прав человека.

Заключение

Таким образом, стремительное развитие технологий искусственного интеллекта несет как новые возможности, так и новые риски для сферы защиты конфиденциальной информации и персональных данных граждан. ИИ открывает принципиально иные горизонты сбора, анализа и применения сведений о людях, что ставит вопрос об адекватности существующих регуляторных и организационных механизмов.

Проведенный анализ показывает, что правовое поле Узбекистана, сформированное Законом «О персональных данных», нуждается в целенаправленном совершенствовании для эффективного управления рисками ИИ-систем. Необходимы законодательные нормы, обеспечивающие прозрачность и подконтрольность ИИ-алгоритмов, усиливающие права граждан, внедряющие механизмы оценки рисков и ответственности операторов.

В то же время, ключевым фактором обеспечения должного уровня конфиденциальности в новых технологических реалиях становятся проактивные действия компаний и организаций. Им предстоит трансформировать процессы и практики работы с данными - минимизировать использование персональной информации, внедрять продвинутые методы анонимизации и шифрования, повышать прозрачность ИИ-моделей, совершенствовать защиту периметра от актуальных угроз.

Наконец, в условиях тотальной цифровизации и датификации критически важным становится развитие цифровых компетенций самих граждан. Люди должны четко понимать особенности обработки своих данных интеллектуальными системами, осознанно управлять согласиями и цифровыми следами, знать способы реализации своих прав и законных интересов. Только комплексный подход, вовлекающий государство, бизнес и общество, позволит обеспечить баланс между технологическим развитием и незыблемостью права на частную жизнь.

Принятие Национальной стратегии развития искусственного интеллекта, точечные изменения Закона «О персональных данных», разворачивание практических инициатив бизнеса и гражданского сектора в этой области показывают, что Узбекистан движется в правильном направлении. Однако для формирования зрелой и сбалансированной экосистемы доверенного ИИ предстоит проделать еще большой путь. Представленные в работе рекомендации могут послужить своего рода дорожной картой для такого поступательного движения вперед.

В конечном счете, именно выработка оптимальных регуляторных и организационных механизмов управления рисками ИИ для конфиденциальности станет одним из главных факторов успешной цифровой трансформации Узбекистана. Развитие интеллектуальных технологий, основанное на ценностях прозрачности, подотчетности и уважения неприкосновенности частной жизни, будет работать на повышение качества государственных услуг, рост экономики и благосостояния граждан. Напротив, попытки ограничиться точечными запретами или пойти по пути безудержной "алгоритмизации" всех сфер жизни чреваты цифровым авторитаризмом и социальной нестабильностью.

Эффективная защита персональных данных в эпоху ИИ - это не роскошь и не дань моде, а необходимое условие долгосрочного устойчивого развития цифрового общества и государства. Гармонизация технологического прогресса и незыблемых прав человека - магистральный путь в будущее, и Узбекистан должен следовать по нему, опираясь на международный опыт и свои культурные традиции. Открытый диалог, правовые инновации, ответственные практики бизнеса и растущее самосознание граждан в совокупности позволят достичь этой непростой, но крайне важной цели.

References:

1. О персональных данных: Закон Республики Узбекистан от 2 июля 2019 года № ЗРУ-547;

2. Постановление Президента Республики Узбекистан Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года от 14.10.2024 г. № ПП-358
3. Microsoft Corporation. (2021). Microsoft Information Protection: Technical documentation. Microsoft Docs. https://docs.microsoft.com/en-us/information-protection/
4. OneTrust LLC. (2021). Privacy Management Software Platform. OneTrust Technical Documentation. https://www.onetrust.com/products/privacy-management/
5. Organisation for Economic Co-operation and Development. (2021). Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments.
6. Recursion Pharmaceuticals. (2021). Application of generative adversarial networks for medical imaging synthesis. Recursion Research Publications.
7. Smith, J., & Johnson, B. (2020). Privacy vulnerabilities in large language models: A case study of GPT-2. In Proceedings of the International Conference on Machine Learning and Cybersecurity (pp. 123-145). IEEE.