КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ДАННЫХ С УЧЕТОМ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАБОЧИХ ПРОЦЕССАХ

Хайдарова Наргизабону Тургунбой кизи
Магистрант Ташкентского государственного юридического университета по направлению «Трудовое право»
Email: davirova.nargizabonu@gmail.com
https://doi.org/10.5281/zenodo.11408148

ARTICLE INFO

Qabul qilindi: 20-May 2024 yil
Ma'qullandi: 25- May 2024 yil
Nashr qilindi: 31- May 2024 yil

KEY WORDS

искусственный интеллект, конфиденциальность, защита данных, современные технологии, кибербезопасности, киберпреступность.

ABSTRACT

В статье исследуются вопросы конфиденциальности и защиты данных в контексте применения искусственного интеллекта (ИИ) в рабочих процессах. Рассматриваются ключевые риски, связанные с обработкой данных с использованием ИИ, а также правовые и этические аспекты, влияющие на конфиденциальность. Анализируются существующие нормативные акты и стандарты, направленные на обеспечение безопасности данных, и приводятся практические рекомендации по минимизации рисков. Статья подчеркивает необходимость разработки комплексных подходов к защите данных в условиях цифровой трансформации рабочих процессов.

Современные технологии искусственного интеллекта (ИИ) проникают во все аспекты нашей жизни, включая рабочие процессы, что приводит к значительным изменениям в управлении данными и вопросах их конфиденциальности. С ростом объема обрабатываемой информации и сложностью алгоритмов, обеспечивающих автоматизацию и оптимизацию рабочих задач, возрастает необходимость особого внимания к защите данных. Важными аспектами становятся не только правовые и регуляторные требования, но и этические вопросы, связанные с правами работников и клиентов на конфиденциальность. Эта статья посвящена рассмотрению ключевых аспектов конфиденциальности и защиты данных в контексте применения ИИ в рабочих процессах. Мы проанализируем основные вопросы, возникающие при использовании ИИ, рассмотрим текущие нормативные требования и предложим практические рекомендации для обеспечения надежной защиты информации и соблюдения прав на конфиденциальность.

Сбор и обработка больших объемов данных. Для обучения и функционирования ИИ-систем требуется сбор и обработка большого объема данных, включая персональные данные сотрудников. Это создает риски утечки данных и их неправомерного использования. Данные могут содержать информацию о производительности, личного характера и других аспектах, которые являются

конфиденциальными и требуют строгой защиты. Но также отметим, что сбор и обработка больших объемов данных с применением ИИ в рабочих процессах открывают широкие возможности для повышения эффективности и качества работы. Однако эти процессы требуют строгого соблюдения норм конфиденциальности, безопасности и этических стандартов. Комплексный подход, включающий внедрение современных технологий защиты данных, регулярный аудит алгоритмов и обучение сотрудников, позволит минимизировать риски и обеспечить ответственное использование ИИ и больших данных в рабочих процессах.

Данные, используемые для ИИ, часто хранятся в облачных сервисах и передаются между различными системами и устройствами. Собранные данные могут быть подвержены кибератакам, утечкам или неправомерному использованию, что ставит под угрозу конфиденциальность сотрудников. Поэтому необходимо внедрять передовые меры кибербезопасности, такие как шифрование данных, анонимизация, а также внедрение строгих политик управления доступом и мониторинга. Компании должны также соблюдать международные стандарты и нормативы, такие как GDPR и CCPA, чтобы обеспечить правовую защиту данных сотрудников.

Использование искусственного интеллекта для мониторинга и анализа производительности сотрудников может существенно повлиять на их право на приватность и создать ощущение постоянного контроля. Современные системы ИИ способны собирать и анализировать обширные данные о рабочих процессах, поведении сотрудников, их взаимодействиях и производительности. Хотя эти технологии могут значительно улучшить управление персоналом и повысить общую эффективность, они также несут в себе ряд рисков. Сбор данных о каждом аспекте работы сотрудников, включая их рабочие привычки, общение с коллегами и даже время, проведенное на перерывах, может восприниматься как вторжение в личную жизнь. Особенно если данные собираются без явного согласия сотрудников или без достаточного объяснения, для каких целей они будут использоваться. Это создает ощущение постоянного наблюдения, что может негативно сказаться на моральном состоянии и удовлетворенности сотрудников. Постоянный мониторинг и анализ могут вызывать стресс и напряжение у сотрудников, так как они могут чувствовать себя под постоянным наблюдением. Это может привести к снижению мотивации, ухудшению рабочей атмосферы и даже к повышенной текучести кадров. Сотрудники могут начать избегать инноваций и творческих решений из-за страха ошибиться и быть негативно оцененными системой.

Для обеспечения конфиденциальности и защиты данных при использовании ИИ важно соблюдать международные и национальные нормативные требования. Самым главным национальным нормативно-правовым актом является Конституция Республики Узбекистан. Часть 3 статьи 31 Конституции Республики Узбекистан гласит – «Каждый имеет право на защиту своих персональных данных, а также требовать исправления недостоверных данных, уничтожения данных, собранных о нем незаконным путем или более не имеющих правовых оснований»[1]. В целях обеспечения более эффективного управления и защиты прав граждан были внесены изменения в Конституцию, направленные на поддержку и развитие цифровых технологий. Эти

[1] Конституция Республики Узбекистан от 1.05.2023 г. (Новая редакция).

изменения подчеркивают важность цифровизации как одного из ключевых направлений государственной политики.

Важно отметить, что с каждым днем уровень преступности в киберпространстве растет и в ответ на возрастающую угрозу киберпреступности и нарушения конфиденциальности персональных данных были ужесточены наказания за нарушение законодательства Республики Узбекистан о персональных данных. Имеется административная и уголовная ответственность за нарушение законодательства о персональных данных. Это включает введение более строгих мер ответственности для юридических и физических лиц, нарушающих правила сбора, систематизации, хранения, изменения, дополнения, использования, предоставления, распространения, передачи, обезличивания и уничтожения персональных данных, а равно несоблюдение при обработке **персональных данных** граждан Республики Узбекистан с использованием **информационных технологий, в том числе во всемирной информационной сети Интернет**, требований по сбору, систематизации и хранению **персональных данных** на технических средствах, физически размещенных на территории Республики Узбекистан, и в базах персональных данных, зарегистрированных в установленном порядке в Государственном реестре баз персональных данных[2]. Данные изменения предусматривают значительные штрафы, что подчеркивает серьезное отношение государства к защите конфиденциальной информации своих граждан.

Международный нормативный акт GDPR (General Data Protection Regulation) является одним из самых строгих нормативных актов по защите данных в мире[3]. Он устанавливает строгие требования к сбору, обработке и хранению персональных данных, включая право на доступ, исправление и удаление данных. GDPR требует, чтобы организации обеспечивали защиту данных **по замыслу и по умолчанию (Privacy by Design and by Default),** что особенно важно при разработке и внедрении ИИ-систем.

Privacy by design. Это означает, что контролер данных обязуется встроить систему защиты данных во все бизнес-процессы (в том числе в процессы разработки продукта или сервиса) на раннем этапе их проектирования и обязуется поддерживать такую систему непрерывно в дальнейшем. Встроенная защита данных **по своему замыслу** — это обязанность заблаговременно предусмотреть защиту персональных данных во всех действиях, начинаниях и решениях компании[4].

Privacy by default. Конфиденциальность по умолчанию подразумевает, что пользователю не нужно предпринимать никакие действия для защиты своей конфиденциальности. Настройки по сохранению конфиденциальности и соответственно защите его персональных данных установлены по умолчанию. Контролеры не должны автоматически полагать, что пользователь дает согласие на обмен данными. Сбору подлежат только те данные, которые необходимы для достижения конкретных целей обработки. Для обеспечения такой

[2] Ст. 46(2) Кодекса об административной ответственности Республики Узбекистан от 22.09.1994 г.
[3] Общий регламент по защите данных и о свободном перемещении таких данных (General Data Protection Regulation). Принят 27 апреля 2016 г. Вступил в силу 25 мая 2018 г.
[4] https://habr.com/ru/companies/digitalrightscenter/articles/479514/

конфиденциальности по умолчанию контролеры должны имплементировать соответствующие технические и организационные меры[5].

Закон Калифорнии о защите персональных данных потребителей California Consumer Privacy Act (CCPA) — это первый комплексный закон о конфиденциальности в США. Он был принят в конце июня 2018 г. и предоставляет различные права на конфиденциальность потребителям Калифорнии. Предприятия, регулируемые CCPA, будут иметь ряд обязательств перед этими потребителями, включая раскрытие информации, общие правила защиты данных (GDPR), подобные права для потребителей, "отказ" для определенных передач данных и требование "согласие" для несовершеннолетних[6]. CCPA предоставляет жителям Калифорнии права на контроль над своими персональными данными, включая право на доступ, удаление и отказ от продажи данных. Компании, работающие с персональными данными калифорнийцев, должны соблюдать требования CCPA, обеспечивая защиту данных и прозрачность их использования.

На основе изученного хотелось бы дать несколько практических рекомендаций для обеспечения конфиденциальности и защиты данных в трудовых отношениях при использовании ИИ:

1) Внедрение политики минимизации данных:

- Собирать только те данные, которые необходимы для конкретных целей, и минимизировать объем обрабатываемой информации.
- Применять методы анонимизации и псевдонимизации данных для снижения риска их неправомерного использования.

2) Использование передовых технологий защиты данных:

- Применять шифрование данных при хранении и передаче, а также внедрять многофакторную аутентификацию и строгие политики управления доступом.
- Регулярно проводить аудит и тестирование систем безопасности для выявления уязвимостей и обеспечения их своевременного устранения.

3) Обеспечение прозрачности и информированности:

- Информировать сотрудников и других заинтересованных сторон о том, какие данные собираются, как они используются и защищаются.
- Обеспечивать возможность доступа к персональным данным и их исправления или удаления по запросу.

4) Соблюдение принципов справедливости и пропорциональности:

- Принимать во внимание права и интересы сотрудников при использовании ИИ для мониторинга и анализа их деятельности.
- Использовать ИИ-системы только в тех случаях, когда это оправдано и не нарушает права на приватность.

5) Обучение и информирование сотрудников:

- Проведение тренингов и семинаров по вопросам защиты данных и кибербезопасности.

[5] https://habr.com/ru/companies/digitalrightscenter/articles/479514/
[6] https://learn.microsoft.com/ru-ru/compliance/regulatory/ccpa-faq

- Обеспечение прозрачности в использовании данных и предоставление сотрудникам информации о том, как их данные используются и защищаются.

В заключение, использование искусственного интеллекта в рабочих процессах представляет как значительные возможности для повышения эффективности и автоматизации, так и серьезные вызовы в области конфиденциальности и защиты данных. Анализ показал, что для минимизации рисков необходимо комплексное и многогранное подходить к обеспечению безопасности данных, включая разработку и соблюдение строгих нормативных актов, внедрение передовых технологий защиты и повышение осведомленности сотрудников о важности защиты данных. Существующие правовые рамки и этические стандарты должны постоянно адаптироваться к быстро меняющимся условиям и технологическим новшествам. Необходимо также усиливать международное сотрудничество для разработки глобально согласованных подходов к регулированию использования ИИ. Важно, чтобы организации активно инвестировали в технологии защиты данных и разрабатывали внутренние политики, направленные на обеспечение конфиденциальности.

Список литературы:

1. Конституция Республики Узбекистан от 1.05.2023 г. (Новая редакция).
2. Кодекс об административной ответственности Республики Узбекистан от 22.09.1994 г.
3. Уголовный кодекс Республики Узбекистан от 22.09.1994 г.
4. Общий регламент по защите данных и о свободном перемещении таких данных (General Data Protection Regulation). Принят 27 апреля 2016 г. Вступил в силу 25 мая 2018 г.
5. https://habr.com/ru/companies/digitalrightscenter/articles/479514/
6. https://learn.microsoft.com/ru-ru/compliance/regulatory/ccpa-faq