Секция «10.5 Компьютерное право и информационная безопасность»

Защита персональных данных в условиях развития систем искусственного интеллекта

Научный руководитель – Зуева Анна Сергеевна

Ховалыг Аюр Шолбанович

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: mongush-8282@mail.ru

Развитие искусственного интеллекта стало одним из ключевых факторов цифровой трансформации. Алгоритмические системы используются в государственном управлении, банковском секторе, медицине, образовании и электронной коммерции. Практически во всех этих сферах они опираются на сбор и анализ информации, значительная часть которой относится к персональным данным.

Персональные данные выступают ресурсом, необходимым для обучения моделей, их тестирования и последующей эксплуатации. Поэтому их защита приобретает не только частноправовое, но и публично-правовое значение, затрагивая конституционные гарантии неприкосновенности частной жизни и доверие общества к цифровым технологиям.

Актуальность темы обусловлена тем, что действующие нормы о персональных данных формировались преимущественно применительно к традиционным информационным системам. Между тем искусственный интеллект характеризуется масштабностью обработки, сложностью алгоритмов, повторным использованием сведений и риском непрозрачности решений. Цель статьи состоит в определении особенностей защиты персональных данных в условиях развития систем искусственного интеллекта и направлений совершенствования правового регулирования.

Особенности обработки персональных данных в системах искусственного интеллекта

Специфика искусственного интеллекта проявляется в высокой зависимости его эффективности от качества и объема данных. Для обучения моделей используются тексты, изображения, аудиозаписи, сведения о поведении пользователей, геолокационные и иногда биометрические данные. Даже при формальном обезличивании совокупность таких сведений нередко позволяет косвенно идентифицировать лицо.

Существенной особенностью является вторичное использование информации. Данные, собранные для оказания услуги, могут применяться для обучения новых моделей, тестирования алгоритмов и коррекции ошибок. Такая практика ставит вопрос о соблюдении принципов целевого ограничения и минимизации обработки.

Еще одна проблема связана с алгоритмической непрозрачностью. При использовании сложных моделей субъект персональных данных часто не способен понять, каким образом его сведения повлияли на итоговое решение системы. Это осложняет реализацию права на информацию об обработке данных и затрудняет контроль за законностью такой обработки.

Проблемы правового регулирования

Общие нормы о персональных данных не всегда позволяют однозначно оценить допустимость конкретных практик использования искусственного интеллекта. Закрепленные в законе принципы законности, соразмерности, ограничения цели и безопасности обработки сохраняют значение, но в алгоритмических системах реализуются сложнее, чем в традиционных базах данных.

Во-первых, затруднения вызывает вопрос согласия субъекта данных. Пользователь может быть уведомлен о факте обработки, но не осознавать, что его сведения будут использоваться не только для предоставления услуги, но и для дальнейшего обучения модели. В результате согласие нередко оказывается формальным.

Во-вторых, проблемным остается автоматизированное принятие решений. Если алгоритм применяется для оценки кредитоспособности, подбора кандидатов или определения условий обслуживания, ошибка модели способна непосредственно затронуть права и законные интересы лица. Оспаривание таких решений осложняется технической сложностью модели и недостаточной прозрачностью критериев оценки.

В-третьих, возрастает риск повторной идентификации личности. Современные методы анализа больших данных позволяют сопоставлять сведения из разных источников и восстанавливать связь между обезличенным набором информации и конкретным человеком. Дополнительную сложность создает трансграничный характер обработки, когда данные одновременно хранятся и анализируются в нескольких юрисдикциях.

Информационная безопасность и защита данных

Защита персональных данных в цифровой среде неразрывно связана с обеспечением информационной безопасности. Для систем искусственного интеллекта это особенно важно, поскольку нарушение конфиденциальности, целостности или доступности данных способно исказить результаты работы модели и повлечь ущерб для широкого круга лиц.

К числу основных угроз относятся несанкционированный доступ к обучающим выборкам, утечки данных, вмешательство в работу алгоритма, подмена входной информации и извлечение сведений о пользователях из параметров модели. Следовательно, правовая защита данных должна включать не только правила получения согласия и определения целей обработки, но и обязательные организационные и технические меры безопасности.

Такие меры охватывают разграничение доступа, шифрование, аутентификацию, журналирование действий, контроль инцидентов, внутренний аудит и оценку рисков. Особое значение имеет подход, при котором защита данных встраивается в архитектуру системы уже на стадии ее проектирования.

Направления совершенствования законодательства

Совершенствование правового регулирования должно носить комплексный характер. Прежде всего необходимо четче определить статус участников обработки данных в экосистеме искусственного интеллекта, разграничив обязанности разработчика модели, оператора сервиса, владельца инфраструктуры и лица, использующего результаты алгоритмической обработки.

Вторым направлением выступает повышение прозрачности алгоритмической обработки. Субъект данных должен понимать, что в отношении него применяется автоматизированная система, какие категории сведений учитываются и как можно оспорить неблагоприятный результат.

Заключение

Развитие систем искусственного интеллекта существенно меняет характер обработки персональных данных и одновременно усиливает требования к их правовой защите. Основная задача состоит не в отказе от действующих правил о персональных данных, а в их адаптации к новым технологическим условиям.

Искусственный интеллект создает риски избыточного сбора информации, вторичного использования сведений, непрозрачности автоматизированных решений, повторной идентификации и нарушений информационной безопасности. В ответ на эти вызовы правовое регулирование должно обеспечивать баланс между развитием цифровых технологий и защитой прав личности.

Эффективная защита персональных данных возможна только при сочетании материально-

правовых гарантий, процедур прозрачности, механизмов контроля и современных технических мер безопасности. Именно комплексный подход способен обеспечить доверие к системам искусственного интеллекта и устойчивость правового порядка в условиях цифровизации.

Источники и литература

1) Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г. с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г.
2) О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ.
3) Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ.
4) Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Рос. Федерации от 1 нояб. 2012 г. № 1119.
5) Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февр. 2013 г. № 21.
6) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
7) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act).