Ломакина Екатерина Олеговна
бакалавр, студентка
Вахтеева Арина Олеговна
бакалавр, студентка
Научный руководитель
Кузнецова Надежда Ильинична
канд. пед. наук, доцент
ФГБОУ ВО «Ульяновский государственный
педагогический университет им. И.Н. Ульянова»
г. Ульяновск, Ульяновская область

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: РИСКИ И ВЫЗОВЫ ДЛЯ КИБЕРБЕЗОПАСНОСТИ

Аннотация: *в статье рассматриваются ключевые проблемы правового регулирования искусственного интеллекта в контексте обеспечения кибербезопасности. Анализируются основные риски, связанные с использованием интеллектуальных систем, включая угрозы утечки данных, автоматизацию кибератак и сложность правовой квалификации действий ИИ. Особое внимание уделяется пробелам в действующем законодательстве и необходимости формирования комплексного подхода к регулированию данной сферы.*

Ключевые слова: *искусственный интеллект, кибербезопасность, информационное право, правовое регулирование, цифровые технологии, защита данных.*

Искусственный интеллект представляет собой совокупность технологий и программных решений, способных имитировать когнитивные функции человека, включая анализ данных, обучение на основе опыта, распознавание образов, принятие решений и прогнозирование. В современном научном дискурсе ИИ рассматривается не только как техническое явление, но и как междисциплинарный феномен, находящийся на стыке информатики, права, философии и социологии [2].

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

С правовой точки зрения одной из ключевых характеристик искусственного интеллекта является его относительная автономность. В отличие от традиционных алгоритмов, функционирующих строго в рамках заранее заданных инструкций, системы ИИ, особенно основанные на методах машинного обучения и нейронных сетей, способны самостоятельно вырабатывать новые модели поведения [1]. Это существенно усложняет процесс определения субъекта ответственности за возможный вред, причинённый в результате функционирования таких систем.

Особое значение имеет способность ИИ к самообучению. В процессе эксплуатации система может изменять свои алгоритмы без прямого вмешательства разработчика, что приводит к так называемому эффекту «непредсказуемости поведения». В юридической практике это порождает проблему установления причинно-следственной связи между действиями разработчика, пользователя и результатом функционирования системы [4]. В ряде случаев невозможно однозначно определить, на каком этапе возникла ошибка – при разработке, обучении или непосредственном применении технологии.

Кроме того, важной особенностью ИИ является его непрозрачность (эффект «чёрного ящика»). Многие современные модели, особенно в области глубокого обучения, не позволяют однозначно интерпретировать логику принятия решений [7]. Это создает серьёзные препятствия для правового контроля, аудита и сертификации таких систем, а также затрудняет использование результатов их работы в качестве доказательств в судебных разбирательствах.

В научной и правовой литературе активно обсуждается вопрос о правовом статусе искусственного интеллекта. Существует несколько подходов к его решению. В рамках первого подхода ИИ рассматривается исключительно как объект права – инструмент, используемый человеком, что предполагает возложение ответственности на разработчика, владельца или оператора системы [3]. Второй подход предполагает возможность признания за ИИ ограниченной правосубъектности, аналогичной юридическим лицам. Однако данная концепция вызывает

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

значительные споры, поскольку ИИ не обладает сознанием, волей и способностью нести ответственность в традиционном юридическом понимании [5].

Отдельного внимания заслуживает проблема разграничения понятий «искусственный интеллект», «автоматизированная система» и «алгоритм». В нормативных актах различных государств отсутствует единое определение ИИ, что приводит к неоднозначности правоприменительной практики [3]. В ряде случаев под ИИ понимаются исключительно самообучающиеся системы, тогда как в других – любые сложные алгоритмы обработки данных.

Стремительное развитие технологий искусственного интеллекта оказывает двойственное влияние на сферу кибербезопасности [2]. С одной стороны, ИИ используется для выявления угроз и защиты информационных систем, с другой – становится мощным инструментом в руках злоумышленников. Применение интеллектуальных алгоритмов в противоправных целях существенно повышает масштаб, скорость и сложность кибератак, формируя новые виды угроз, к которым традиционные механизмы защиты оказываются недостаточно подготовленными [5].

Использование искусственного интеллекта позволяет злоумышленникам автоматизировать ключевые этапы кибератак, включая разведку, выявление уязвимостей и эксплуатацию слабых мест информационных систем. В отличие от традиционных атак, требующих значительного участия человека, ИИ способен самостоятельно анализировать сетевую инфраструктуру, выявлять потенциальные точки входа и подбирать наиболее эффективные способы их использования [8].

Особую опасность представляют так называемые адаптивные атаки, при которых алгоритмы машинного обучения изменяют стратегию поведения в зависимости от реакции защитных систем [4]. Это делает такие атаки более устойчивыми к обнаружению и блокировке. Кроме того, ИИ может использоваться для создания полиморфного вредоносного программного обеспечения, которое изменяет свой код, обходя антивирусные средства и системы обнаружения вторжений [3].

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Дополнительным фактором риска является снижение порога входа в киберпреступность. Благодаря доступности инструментов на основе ИИ даже лица с ограниченными техническими навыками могут осуществлять сложные атаки, используя готовые алгоритмы и программные решения [7].

Современные системы искусственного интеллекта функционируют на основе обработки значительных массивов данных, включая персональные, биометрические и иные чувствительные сведения [3]. Это делает их привлекательной целью для киберпреступников. Нарушение безопасности таких систем может привести к масштабным утечкам информации, последствия которых затрагивают как отдельных пользователей, так и организации и государственные структуры [6].

Кроме того, существует риск так называемого «отравления данных» (data poisoning), при котором злоумышленник внедряет искажённые или вредоносные данные в обучающую выборку [1]. Это может привести к некорректной работе системы, снижению точности её решений или созданию уязвимостей, которые впоследствии будут использованы для атак.

Искусственный интеллект активно используется для создания и распространения дезинформации. Одним из наиболее опасных проявлений данного риска являются технологии генерации синтетического контента, включая «глубокие подделки» (deepfakes). С их помощью возможно создание реалистичных изображений, аудио- и видеоматериалов, имитирующих действия и высказывания реальных лиц [8].

Дополнительно ИИ используется для автоматизации социальной инженерии. Генеративные модели позволяют создавать персонализированные фишинговые сообщения, адаптированные под конкретного пользователя, что значительно повышает вероятность успешного обмана [6]. В результате традиционные методы распознавания мошенничества становятся менее эффективными.

Одной из фундаментальных проблем, связанных с использованием искусственного интеллекта, является непрозрачность его функционирования. Многие

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

современные модели, особенно основанные на глубоких нейронных сетях, представляют собой сложные системы, внутренняя логика которых трудно поддаётся интерпретации [4].

Одной из ключевых проблем является определение субъекта ответственности за действия ИИ. Возможными субъектами могут выступать разработчики, владельцы или пользователи системы, однако четкое разграничение их ответственности отсутствует [8].

Темпы развития технологий значительно опережают развитие правовых норм. Это приводит к возникновению правовых пробелов, которыми могут воспользоваться злоумышленники [3].

Несмотря на наличие норм о защите персональных данных, вопросы использования данных в системах ИИ остаются недостаточно урегулированными, особенно в части трансграничной передачи информации.

В различных странах предпринимаются попытки регулирования ИИ и связанных с ним рисков. Основные направления включают: разработку этических принципов использования ИИ; установление требований к прозрачности алгоритмов; усиление контроля за обработкой персональных данных; создание специализированных органов по контролю за цифровыми технологиями [5].

Международные организации также разрабатывают рекомендации, направленные на обеспечение безопасного и ответственного использования ИИ. Однако данные меры носят преимущественно рекомендательный характер [2].

Для эффективного противодействия киберугрозам необходимо формирование комплексной системы правового регулирования, включающей:

– разработку специализированного законодательства в сфере ИИ;

– установление четких критериев ответственности за вред, причиненный ИИ;

– введение обязательных требований к безопасности алгоритмов;

– развитие международного сотрудничества в области кибербезопасности;

– создание механизмов аудита и сертификации систем ИИ [4].

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Особое значение имеет внедрение принципа «безопасность по проекту», предполагающего учет требований кибербезопасности на этапе разработки технологий [7].

Искусственный интеллект представляет собой мощный инструмент, способный как повысить уровень кибербезопасности, так и создать новые угрозы. Формирование эффективной нормативной базы требует комплексного подхода, объединяющего усилия государства, бизнеса и научного сообщества [4]. Только при наличии сбалансированной системы регулирования возможно обеспечить безопасное и устойчивое развитие цифровой среды.

Список литературы

1. Бабенкова В.Р. Искусственный интеллект как часть общественной жизни: этико-правовые проблемы и пути их решения / В.Р. Бабенкова, Н.В. Кравченко // Актуальные проблемы государства и права. – 2024. – Т. 8. №1 (29). – С. 7–16. – DOI 10.20310/2587-9340-2024-8-1-7-16. EDN OXCDEC

2. Баранов А.А. Искусственный интеллект и право: современные вызовы / А.А. Баранов // Журнал российского права. – 2023. – №5. – С. 45–56.

3. Бачило И.Л. Информационное право: учебник / И.Л. Бачило. – М.: Юрайт, 2022. – 522 с.

4. Войниканис Е.А. Право и искусственный интеллект: вопросы теории / Е.А. Войниканис . – М.: Статут, 2020. – 304 с.

5. Громов В.В. Кибербезопасность и правовые механизмы защиты информации / В.В. Громов // Информационное право. – 2022. – №3. – С. 12–19.

6. Ершов В.В. Цифровая трансформация права в условиях развития ИИ / В.В. Ершов // Государство и право. – 2023. – №2. – С. 33–41.

7. Жуков В.И. Естественный и искусственный интеллект: диалектика взаимодействия и правовые регуляторы девиаций / В.И. Жуков, Г.С. Жукова // Государство и право. – 2023. – №6. – С. 136–148. – DOI 10.31857/S102694520025956–2. EDN APNBSV

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

8. Зорькин В.Д. Право в цифровом мире: монография. – М.: Норма, 2021. – 480 с.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)