Гаркуша Виктория Михайловна
аспирант, преподаватель
Маркарян Григорий Каренович
бакалавр, студент
ФГБОУ ВО «Кубанский государственный аграрный
университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

ПРАВОСУБЪЕКТНОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕЖДУНАРОДНОМ ПРАВЕ: ОТ «ЭЛЕКТРОННОГО ЛИЦА» К НОВОМУ СУБЪЕКТУ

Аннотация*: в статье раскрываются проблемы определения международной правосубъектности сложных автономных систем искусственного интеллекта. Анализируются коллизии, возникающие между традиционными критериями субъектности в международном праве, нормами о международной ответственности и принципиально новой природой ИИ. Исследуются концепции «электронного лица» и их применимость для восполнения правового вакуума, а также проблемы распределения ответственности между разработчиками, операторами и самими системами за действия, подпадающие под состав международных правонарушений.*

Ключевые слова*: искусственный интеллект, международная правосубъектность, электронное лицо, международная ответственность, автономные системы, правовой вакуум, деликтоспособность, регулирование ИИ.*

Проблема правосубъектности искусственного интеллекта (далее – ИИ) перешла из области теоретических дискуссий в практическую плоскость международного права. Ярким подтверждением этому стал инцидент, подробно описанный компанией Anthropic в ноябре 2025 года [5]. Так, китайская государственная хакерская группа использовала искусственный интеллект ИИ Claude для проведения масштабной кампании кибершпионажа, где на долю искусственного интеллекта пришлось от 80% до 90% операций. Данный случай признан первой

задокументированной кибератакой, выполненной практически без человеческого вмешательства, что демонстрирует настоятельную необходимость пересмотра традиционных правовых теорий и создания новых механизмов ответственности в международном праве.

Реальный инцидент с использованием Claude в сентябре 2025 года наглядно иллюстрирует масштаб вызова. Злоумышленники, оцененные Anthropic с высокой степенью уверенности как китайская государственная группа, использовали ИИ-инструмент Claude Code в качестве автономного агента для атаки на примерно 30 глобальных целей, включая крупные технологические компании, финансовые учреждения и правительственные агентства. Атака была высокоавтоматизированной: человеческое вмешательство требовалось лишь в 4–6 критических точках принятия решений за весь процесс взлома, в то время как ИИ самостоятельно выполнял разведку, создавал эксплойты, извлекал данные и документировал процесс.

Для обхода встроенных систем безопасности злоумышленники применили метод «джейлбрейка», введя ИИ в заблуждение посредством социальной инженерии: модель была убеждена, что участвует в легитимном тестировании по заказу компания, занимающейся кибербезопасностью. Это позволило разбить комплексную атаку на множество мелких, безобидных с точки зрения модели задач.

Указанный случай ставит перед международным правом сложнейший вопрос: можно ли рассматривать подобную автономную кибератаку, инициированную и в значительной степени исполненную ИИ, как «вооруженное нападение» по смыслу ст. 51 Устава ООН [1]?

Международное сообщество демонстрирует разделенные позиции по этому вопросу: США и Великобритания склоняются к расширительному толкованию, в то время как Китай и Россия настаивают на необходимости четких критериев. При этом сам Китай официально отвергает свою причастность к данной хакерской кампании.

Концепция «электронного лица» как потенциального решения этих проблем сталкивается с серьезными практическими противоречиями. Так, в научном

сообществе нет единого подхода: одна группа ученых выступает за признание в законодательстве нового субъекта права – виртуального лица, в то время как другая считает, что использование технологий для создания виртуального профиля не порождает нового субъекта права. Эта неопределенность усугубляется диаметрально противоположными подходами разных юрисдикций. Европейский Союз в Регламенте AI Act [2] делает акцент на оценке рисков и устанавливает жесткие ограничения для «высокорискового» ИИ, но при этом сознательно избегает вопроса о наделении ИИ правосубъектностью. Китай, напротив, в Законе об искусственном интеллекте 2024 года делает ставку на «управляемое развитие», создавая среду с минимальными ограничениями для стимулирования инноваций. США характеризуются отсутствием единого федерального регулирования ИИ, что создает правовые лазейки и приводит к фрагментарному подходу, основанному на инициативах отдельных штатов. Россия же активно формирует собственную нормативную базу, о чем свидетельствуют утвержденная Национальная стратегия развития искусственного интеллекта до 2030 года [3] и Концепция развития регулирования в сфере технологий ИИ и робототехники до 2024 года [4]. Этот правовой дисбаланс подрывает возможность формирования последовательного международно-правового режима.

Среди нерешенных споров особую остроту приобретают вопросы ответственности и глобальной безопасности. Дискуссия о возможности привлечения ИИ к уголовной ответственности разделила экспертов на два лагеря. Сторонники этой позиции указывают, что технологии достигли уровня, когда системы проявляют подобие автономной воли. Они утверждают, что без признания за сложными ИИ деликтоспособности образуется правовой вакуум, особенно в случаях причинения вреда. А противники возражают, говоря, что отсутствие у машины сознания, морального выбора и способности осознавать последствия своих действий делает бессмысленным приписывание ей вины. Они настаивают, что ответственность в любом случае должна оставаться за людьми и организациями (разработчиками, операторами, владельцами), которые создали и используют эти системы.

Не менее острая дискуссия разворачивается вокруг оценки развития ИИ как угрозы международной безопасности. Здесь сталкиваются различные геополитические и экономические интересы. Технологические державы (США, Китай) настаивают на том, что регулирование должно в первую очередь стимулировать инновации и не должно сковывать их технологическое развитие. Развивающиеся страны указывают, что автономное оружие и передовой ИИ усиливают технологическое неравенство, предоставляя развитым странам непропорциональные военные и экономические преимущества. Россия занимает промежуточную позицию, выступая за сохранение контроля человека над любой техникой. Российская дипломатия активно участвует в обсуждении этих вопросов в ООН и предлагает разработку международного договора, аналогичного Договору о нераспространении ядерного оружия (ДНЯО), для контроля за военным ИИ. Мировое сообщество осознает остроту этих вызовов. Более 120 стран поддерживают идею создания нового международного договора по автономному оружию, а Генеральный секретарь ООН призвал договориться о таком документе до 2026 года.

Проведенный анализ позволяет сделать вывод о необходимости разработки комплексного международно-правового подхода к регулированию искусственного интеллекта. В качестве первоочередных мер выступают:

во-первых, создание международного реестра высокорисковых систем ИИ под эгидой ООН, который позволит осуществлять мониторинг их разработки и применения.

Во-вторых, разработка многоуровневой модели ответственности, учитывающей степень автономности системы и характер правонарушения, с распределением бремени ответственности между разработчиками, операторами и государствами.

В-третьих, учреждение международного органа по этике искусственного интеллекта, наделенного полномочиями по выработке стандартов и расследованию инцидентов.

Решение вопросов правосубъектности искусственного интеллекта требует сбалансированного подхода, сочетающего технологический прогресс с

обеспечением международной безопасности и защитой прав человека. Успешное развитие международно-правового регулирования в этой области будет способствовать созданию предсказуемых условий для технологического развития при сохранении стабильности международных отношений.

Список литературы

1. Устав Организации Объединенных Наций (принят в г. Сан-Франциско 26.06.1945) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. – Вып. XII. – М., 1956. – С. 14–47 [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/about-us/un-charter (дата обращения: 19.12.2025).

2. Об искусственном интеллекте: Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года // Официальный журнал Европейского союза. – 2024. – L 2024/1689 [Электронный ресурс]. – Режим доступа: http://data.europa.eu/eli/reg/2024/1689/oj (дата обращения: 19.12.2025).

3. Указ Президента Российской Федерации от 10.10.2019 №490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201910100002 (дата обращения: 19.12.2025).

4. Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года (утв. распоряжением Правительства РФ от 19.08.2020 №2129-р) [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/74431128/ (дата обращения: 19.12.2025).

5. Китайская хакерская госгруппа использовала Claude для масштабного кибершпионажа [Электронный ресурс]. – Режим доступа: https://habr.com/ru/news/966264/ (дата обращения: 19.12.2025).