DOI 10.35775/PSI.2026.126.2.039
УДК 32.327

И.В. ЯРЕМЧУК
аспирант, Московский государственный
университет имени М.В. Ломоносова,
Россия, г. Москва
E-mail: ffww4357@mail.ru

АЛГОРИТМЫ И ПРАВДА: КАК ЕС РЕГУЛИРУЕТ ИИ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Актуальность данного исследования определяется действительным фактом общественного развития – проникновение искусственного интеллекта во все сферы общественно-политической жизни общества, что объективно порождает новые вызовы в сфере общественной безопасности. Цифровая трансформация общества открывает возможности для его развития, но и создает инструменты для масштабной политической манипуляции, распространения дезинформации и подрыва общественного доверия через такие технологии, как дипфейки и алгоритмически генерируемый контент. Объект исследования – политика Европейского союза в сфере регулирования искусственного интеллекта и цифрового пространства в контексте цифровой трансформации. Предмет исследования – конкретные нормативно-правовые акты и инициативы ЕС (AI Act, Digital Services Act, Кодекс практики по дезинформации), направленные на минимизацию рисков, связанных с использованием искусственного интеллекта для подрыва общественной и политической стабильности. Результаты исследования заключаются в последовательном системном анализе европейского подхода к регулированию ИИ, выявлении его ключевых инструментов, таких как требование прозрачности контента и управления рисками, а также в оценке потенциальных пробелов и проблем внедрения данного регулирования, включая вопросы защиты фундаментальных прав и сохранения технологического потенциала цифровой среды хозяйствования.

Ключевые слова: *цифровое общество, искусственный интеллект, законотворчество, политическая идеология, управление рисками, общественное сознание, социальный скоринг.*

Введение. Искусственный интеллект (ИИ) в современном публичном дискурсе окружен множеством мифов и полярных оценок, варьирующихся от утопических ожиданий тотального прогресса до антиутопических страхов перед неподконтрольным разумом: «**Например, существует миф о «умных» машинах, способных обрести собственное сознание и разум, что нередко ассоциируется с историями о живых роботах или искусственных существах, оживленных в результате технического трансформации. Этот мифологический образ отражает общесоциальные опасения и страхи перед потерей контроля над технологическим развитием**» [4. С. 554]. Метафора «алгоритмы и правда», вынесенная в Заголовок исследования, отражает один из центральных

конфликтов в современном общественном сознании – противостояние между объективной реальностью, фактологическим базисом публичной сферы и алгоритмическими системами, способными эту реальность симулировать, искажать или подменять. Как безусловно верно отметил Жан Бодрийяр: «**В этом состоит секрет дискурса, который больше не является лишь неоднозначным, как это случается с политическим дискурсом, но выражает невозможность определить позицию власти, невозможность определить позицию в дискурсе. И эта логика не склоняется ни в ту, ни в другую сторону. Она пронизывает все дискурсы вопреки их желаниям**» [2. С. 28]. Алгоритмы, лежащие в основе социальных сетей и систем генеративного ИИ, становятся не просто инструментами обработки информации, а арбитрами ее распространения, видимости и, в конечном счете, социального конструирования политической реальности, что порождает фундаментальную проблему для политической науки и практики того, как обеспечить целостность публичного пространства в условиях, когда технологическая возможность создания убедительной лжи превышает скорость и возможности человеческой верификации своего места в цифровом мире. Теоретическая значимость данного исследования заключается в попытке эвристической концептуализации ответа Европейского союза на указанный вызов через призму регуляторного подхода, основанного на управлении рисками и защите базовых аксиологических ценностей общества. Данное исследование позволяет перевести дискуссию о политических последствиях ИИ из плоскости технологического детерминизма в плоскость институционального анализа, показав, как наднациональные структуры адаптируются к новым угрозам. Поэтому анализ европейского опыта важен именно для понимания формирующейся глобальной парадигмы цифрового управления, в которой баланс между цифровизацией, безопасностью и правами человека становится ключевым полем политической борьбы и нормотворчества.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [3; 5; 6; 7; 8; 10; 12; 14; 16; 19].

Однако исследование политики Европейского союза в сфере регулирования искусственного интеллекта и цифрового пространства в контексте цифровой трансформации нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Основная часть. Проблематика политических рисков, связанных с искусственным интеллектом, наиболее остро проявляется в сфере информационного воздействия. ИИ, в особенности его генеративные формы, становится основой для массового производства дезинформации, создания дипфейк-видео, имитирующих публичных фигур и тонкой настройки микромасштабной политической рекламы, манипулирующей восприятием избирателей: «**Речь идет о новейших возможностях манипуляции сознанием избирателей (в широком смысле – любых реципиентов политических коммуникаций) и их дезинформации,**

которые влекут за собой применение искусственного интеллекта» [17. С. 46]. Социальные сети, чьи бизнес-модели построены на вовлечении пользователей, зачастую непреднамеренно становятся катализаторами распространения такого контента, поскольку алгоритмы рекомендаций отдают приоритет эмоционально заряженным и конфликтным материалам с часто алогичным содержанием, которое создает прямую угрозу электоральным процессам, общественному доверию к медиа и государственным институтам, а в долгосрочной перспективе самой идее рационального публичного обсуждения, основанного на общей фактологической основе. Дипфейки, используемые в политических целях для компрометации кандидатов или распространения ложных заявлений от их имени, обладают потенциалом мгновенной дестабилизации политической обстановки, подрывая саму возможность проведения свободных и честных выборов: «**...нейросети создают и поддерживают определенный дискурс, который может быть использован для манипулирования общественным мнением и конструирования новой реальности. С ростом влияния этих технологий множатся угрозы формирования искусственной среды, в которых манипуляторы способны направлять коллективные представления и восприятие в нужное русло. Это актуализирует вопросы о подлинности и достоверности создаваемой информации и увеличивает риски искажения представлений о действительности**» [15. С. 630]. Ответ Европейского союза на эти вызовы сформировался как многоуровневая экосистема регуляторных актов, дополняющих друг друга, в котором базовый элемент – это Кодекс практики по дезинформации (3) (2022 года). Хотя определенной своей частью этот документ следствие общей мировой геополитической обстановки, в которой ЕС гиперболизировано создают симулякры угроз, тем не менее он устанавливает важные стандарты прозрачности в отношении политической рекламы, действий по противодействию вредоносным ботам и координации в кризисных ситуациях, таких как выборы или вооруженные конфликты. Более жестким регулирующим инструментом выступает Регламент Digital Services Act (DSA (4)): «**Дальнейшие планы Еврокомиссии по цифровому реформированию ЕС до 2030 г. представлены в сообщении о Цифровом компасе от 09.03.2021...В некоторой части эти планы были реализованы с разработкой Регламента об управлении данными (European Data Governance Act), Регламента о цифровых услугах (Digital Services Act)26, Регламента о цифровых рынках (Digital Markets Act) и новой Стратегии кибербезопасности (Cybersecurity Strategy)**» [11. С. 96]. Вступивший в полную силу в 2024 году DSA вводит обязанность для действительно крупных онлайн-платформ и поисковых систем системно оценивать риски, которые их платформы представляют для общества, включая риски манипуляций, распространения дезинформации и нарушения фундаментальных прав, то есть платформы обязаны принимать меры по снижению этих рисков, предоставлять данные независимым исследователям и соблюдать строгие правила в отношении таргетированной рекламы, включая запрет на таргетинг по особо чувствительным данным.

Ключевым элементом в борьбе с манипулятивным контентом, порождаемым ИИ, становятся инициативы по обеспечению прозрачности и «traceability» [20. С. 164-173] (рус. трейсабильности – прослеживаемости). В рамках действующего законодательства ЕС это означает требование к разработчикам создавать ИИ-системы таким образом, чтобы обеспечивалась объяснимость их решений, пользователь должен понимать, взаимодействует ли он с искусственным интеллектом, что находит прямое отражение в Регламенте об искусственном интеллекте (AI Act (1)) – краеугольном камне европейского подхода, который вводит обязательную маркировку контента, сгенерированного ИИ, особенно в случаях, когда существует риск введения в заблуждение. Для систем, классифицированных как системы высокого риска (к которым могут относиться и некоторые системы, используемые в избирательном процессе), установлены строгие требования к качеству данных, технической документации, ведению журналов событий (логов) и человеческому надзору. Принцип «трейсабильности» подразумевает, что должна существовать возможность проследить, какие данные и на каком этапе повлияли на решение или выход системы, что критически важно для расследования инцидентов, связанных, например, с дипфейками.

Этическое регулирование ИИ в ЕС не сводится только к запретительным мерам, а встроено в более широкую нормативную рамку, основанную на политике общественного развития. Еще до принятия AI Act Европейская комиссия разработала «Этические руководящие принципы для надежного ИИ» (2), основанные на ключевых принципах организации человеческой активности в цифровой среде – человеческий надзор и контроль, техническая надежность и безопасность, конфиденциальность и управление данными, прозрачность, разнообразие, недискриминация и справедливость, социальное и экологическое благополучие, а также подотчетность. AI Act операционализирует эти принципы, переводя их в юридически обязательные требования для разных категорий риска, то есть этика в европейской модели перестает быть факультативной рекомендацией и становится предметом правоприменения. Рассмотрим основные положения Al Act по содержанию – таблица 1.

Таблица 1. Основные положения Регламента Европейского союза об искусственном интеллекте (AI Act)

Положение	Содержание и значение
Подход, основанный на уровне риска	Системы ИИ разделены на четыре категории: 1) Недопустимый риск (запрещены, например, «*социальный скоринг*» [9. С. 96-101] государством, системы манипуляции с использованием уязвимостей). 2) Высокий риск (строгие предварительные требования к соответсвию следующим критериям: оценка соответствия, качество данных, документация, прозрачность, человеческий надзор, кибербезопасность; сюда входят ИИ в управлении критической инфраструктурой, образовании, правоприменении, избирательных процессах). 3) Ограниченный риск (обязательства по прозрачности, например, четкое информирование пользователя о взаимодействии с ИИ, маркировка дипфейков). 4) Минимальный или нулевой риск (применяются без ограничений, например, спам-фильтры).
Требования к прозрачности (Transparency)	Для систем ИИ, взаимодействующих с людьми (чат-боты, эмоциональный анализ), пользователи должны быть проинформированы, что общаются с машиной. Обязательная маркировка **синтетического контента** (изображения, аудио, видео), созданного с помощью ИИ. Разработчики генеративных ИИ (например, большие языковые модели) обязаны раскрывать, что контент сгенерирован ИИ, публиковать подробные сводки об использовании охраняемых авторским правом данных для обучения.
Требования к управлению и данным	Для систем **высокого риска** обязательно наличие системы управления рисками на протяжении всего жизненного цикла, использование высококачественных, репрезентативных и размеченных наборов обучающих данных для минимизации смещений и дискриминационных результатов. Обязательное ведение автоматизированных журналов событий (логирование) для обеспечения прослеживаемости решений.
Правила для поставщиков и пользователей	**Поставщики** (разработчики) систем высокого риска несут ответственность за соблюдение предварительных требований и процедуру оценки соответствия. **Пользователи** обязаны использовать системы в соответствии с инструкциями, проводить мониторинг их работы, обеспечивать человеческий надзор и информировать о рисках.
Надзор и правоприменение	Создание **Европейского управления по искусственному интеллекту** при Комиссии ЕС для координации. Национальные надзорные органы будут осуществлять мониторинг и правоприменение. Установлены значительные штрафы за нарушения: до 35 млн евро или 7% глобального годового оборота компании.

Источник: разработано автором.

AI Act представляет собой первую в мире комплексную правовую рамку для регулирования ИИ, построенную на принципе пропорциональности угроз, ядром которой является классификация по уровню риска, которая направляет наиболее строгие регуляторные меры (предварительное соответствие, аудит) на те системы ИИ, которые представляют наибольшую угрозу для безопасности, прав и политических процессов граждан ЕС. При этом сам акт напрямую нацелен проблему дезинформации через обязательную прозрачность и маркировку синтетического контента, стремясь дать пользователям инструмент для критического восприятия информации, что является следствием политических решений в части переориентации субсидирования бюджетных средств на общеевропейские блага (цифровые, связь и т.д.): «**Эволюция бюджетных приоритетов ЕС подтверждает тезис о постепенной переориентации с субсидий сельскому хозяйству на обеспечение общеевропейских благ**» [13. С. 2].

Несмотря на новаторский характер AI Act и общий подход ЕС сталкиваются с рядом проблем и имеют очевидные недостатки, так остается вопрос эффективного правоприменения в отношении глобальных технологических гигантов и быстро развивающихся проектов с открытым кодом (англ. open-source), когда код открытый и им может пользоваться и изменять для своих нужд каждый пользователь, как осуществлять мониторинг? Техническая сложность аудита «черных ящиков» нейросетей, особенно фундаментальных моделей, остается нерешенной проблемой в рамках AI Act. Существует риск гиперрегуляции, которая может затормозить развитие цифровой среды в Европе и привести к «бегству» разработчиков в другие юрисдикции с более мягкими правилами [1]. Само определение «высокого риска» может быть предметом лоббирования и со временем потребует пересмотра, так как технологии эволюционируют и опять возникает проблема политического лоббирования в рамках двух взаимоисключающих парадигм – индивидуализм и коллективизм: «**Индивидуализм и коллективизм – это естественные антагонисты, которые аксиоматичны и определяют онтологические и гносеологические различия большинства общественных, гуманитарных теорий, концепций, практик. В том числе сущностный смысл почти всех остальных традиционных ценностей**» [18. С. 138]. Акцент на предварительном соответствии уровня риска может создать высокий барьер для входа на рынок для стартапов и малого бизнеса, так как несмотря на декларируемую цель защиты фундаментальных прав, критический анализ позволил обнаружить потенциальные лазейки, особенно в области правоохранительного и миграционного использования ИИ (например, систем биометрической идентификации в реальном времени в общественных местах), где исключения могут подорвать права на частную жизнь и свободу собраний.

Заключение. Политика Европейского союза в области регулирования искусственного интеллекта в эпоху цифровой трансформации общественного пространства представляет собой масштабный эксперимент по институционализации технологического прогресса. ЕС подходит к проблеме «алгоритмов и правды» не как к узкотехнической, а как к системной политической угрозе целостности

публичной сферы, когда ответ формируется комплексно – через укрепление ответственности цифровых платформ (DSA), создание отраслевых стандартов сотрудничества (Кодекс по дезинформации) и, наконец, установление всеобъемлющих горизонтальных правил для разработки и внедрения самих технологий ИИ (AI Act). Центральными элементами этой стратегии являются принципы управления рисками, прослеживаемости решений и прозрачности происхождения контента, что напрямую направлено на противодействие политическим манипуляциям с помощью дипфейков и таргетированной дезинформации. Тем не менее европейский путь регулирования является не окончательным решением, а тем более оптимальным решением, а скорее динамически развивающейся инициативой, отражающей попытку найти баланс между политической волей, идеологией и общественным мнением. Выявленные недостатки, такие как проблемы правоприменения, риски гиперрегуляции и потенциальные лазейки в области прав человека, указывают на то, что процесс регулирования будет продолжать эволюционировать под давлением технологических прорывов, политических кризисов и общественной дискуссии. Опыт ЕС показывает, что в условиях, когда алгоритмы становятся активными агентами в производстве и распространении информации (и дезинформации), классические политические институты вынуждены развивать новые компетенции и инструменты, так как регулирование ИИ перестает быть вопросом исключительно технических стандартов, превращаясь в поле напряженной политической борьбы за будущее публичного пространства, доверия и самой истины. Успех европейской модели будет зависеть не только от буквы закона, но и от способности наднациональных и национальных институтов адаптироваться к непредсказуемой цифровой реальности, создаваемой цифровой трансформацией общества.

ПРИМЕЧАНИЯ:

(1) AI Act // https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

(2) Ethics guidelines for trustworthy AI // https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

(3) The 2022 Code of Practice on Disinformation // https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

(4) The Digital Services Act package // https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Байниязова З.С.** Проблема консолидации правового статуса личности в российской правовой системе в цифровую эпоху / З.С. Байниязова, А.В. Бондаренко, М.Ю. Лукиянов // Евразийский юридический журнал. 2024. № 1 (188). С. 14-17. EDN ITCXPS.

2. **Бодрийяр Ж.** Симулякры и симуляции / [пер. с фр. А. Качалова]. М.: Издательский дом «ПОСТУМ», 2015. 240 с. (Технология свободы).
3. **Гавров С.Н., Еремкин М.П.** Использование искусственного интеллекта в контексте информационной войны // Вопросы политологии. 2025. № 2.
4. **Гибадуллин А.А.** Мифы и легенды вокруг искусственного интеллекта, мифология искусственного интеллекта // Академическая публицистика. 2024. № 1-1. EDN HHGUUP.
5. **Гребенщикова Д.Е.** Роль социальных сетей и альтернативных медиа в изменении медиаобраза России на примере работы SPUTNIK // Вопросы политологии. 2025. № 12.
6. **Крюкова Е.В.** Двойственный характер использования интернет-технологий как инструмента взаимного контроля государства и общества // Вопросы национальных и федеративных отношений. 2025. № 12.
7. **Кубанцева Е.В.** Индекс цифровой независимости как инструмент оценки суверенитета государства в условиях цифрового неоколониализма // Вопросы политологии. 2026. № 1.
8. **Медведев Н.П.** Современные выборы и проблемы цифровизации общественно-политической жизни // Вопросы политологии. 2025. № 12.
9. **Минбалеев А.В.** Проблемы социальной эффективности и защиты прав человека при использовании искусственного интеллекта в рамках социального скоринга // Вестник Южно-Уральского государственного университета. Серия: Право. 2020. Т. 20, № 2. DOI 10.14529/law200216. EDN FITGSX.
10. **Москвичев В.Р., Ершова Л.В.** Цифровые медиа как фактор трансформации политического лидерства в XXI веке // Вопросы политологии. 2026. № 1.
11. **Панфилов П.О.** Правовое регулирование деятельности онлайн-платформ на едином цифровом рынке ЕС: возможности для ЕАЭС // Lex Russica (Русский закон). 2023. Т. 76, № 2 (195). DOI 10.17803/1729-5920.2023.195.2.091-100. EDN EYBGZS.
12. **Пин Фэн, Зайнуллин С.Б.** Риски и меры противодействия цифровой трансформации предприятия в современном мире // Евразийский Союз: вопросы международных отношений. 2025. № 2.
13. **Примак А.В.** Многолетняя финансовая рамка 2028-2034 и общеевропейские общественные блага: как бюджетное увеличение до 1,7% ВНД может преобразить федерализм ЕС / А.В. Примак, М.С. Набойченко, К.Д. Кудряшова // Human Progress. 2024. Т. 10, № 11. DOI 10.46320/2073-4506-2024-11a-35. EDN FSUIAT.
14. **Серохвостов В.В.** Возможности и угрозы применения искусственного интеллекта в политическом имиджмейкинге // Вопросы политологии. 2025. № 12.
15. **Соколов А.В., Фролов А.А., Бабаджанян П.А.** Применение технологий искусственного интеллекта в политике: угрозы и возможности // Вестник Российского университета дружбы народов. Серия: Политология. 2025. Т.

27. № 3 // С. 622-637 https://cyberleninka.ru/article/n/primenenie-tehnologiy-iskusstvennogo-intellekta-v-politike-ugrozy-i-vozmozhnosti.
16. **Сюй Чан.** The Reconstruction of World Order in the Digital Age: Technological Power, Rule Game, and New Geopolitical Landscape/Трансформация мирового порядка в цифровую эпоху: технологическая мощь, правила игры и новый геополитический ландшафт // Вопросы политологии. 2025. № 9.
17. **Уртаева Э.Б.** Возможности и угрозы применения искусственного интеллекта (ИИ) в политических коммуникациях // Общество: политика, экономика, право. 2024. № 2 (127). DOI 10.24158/pep.2024.2.3. EDN UALQLW.
18. **Хайруллин В.А.** Экономика и социология человеческого развития / В.А. Хайруллин, И.А. Кулькова, Э.Н. Ямалова // Дискуссия. 2024. № 8 (129). С. 124-142. DOI 10.46320/2077-7639-2024-8-129-124-00. EDN LZQPZT.
19. **Шкурина С.С.** Влияние информационно-коммуникационных технологий на современные общественно-политические процессы // Региональное и муниципальное управление: вопросы политики, экономики и права. 2025. № 2.
20. **Schwägele F.** Traceability from a European perspective // Meat science. 2005. Т. 71. № 1. DOI 10.1016/j.meatsci.2005.03.002.

I.V. IAREMCHUK
Postgraduate, Lomonosov Moscow State University, Moscow, Russia

ALGORITHMS AND TRUTH: HOW THE EU REGULATES AI IN THE AGE OF DIGITAL TRANSFORMATION

The relevance of this study is determined by a real fact of social development: the penetration of artificial intelligence into all spheres of socio-political life, which objectively creates new challenges to public security. The digital transformation of society opens opportunities for its development, but also creates tools for large-scale political manipulation, the spread of disinformation, and the undermining of public trust through technologies such as deepfakes and algorithmically generated content. The object of this study is the European Union's policy on regulating artificial intelligence and the digital space in the context of digital transformation. The subject of the study is specific EU regulations and initiatives (AI Act, Digital Services Act, Code of Practice on Disinformation) aimed at minimizing the risks associated with the use of artificial intelligence to undermine social and political stability. The study's results include a systematic analysis of the European approach to AI regulation, identifying key tools such as content transparency and risk management requirements, and assessing potential gaps and challenges in implementing this regulation, including issues of protecting fundamental rights and preserving the technological potential of the digital economic environment.

Key words: *digital society, artificial intelligence, lawmaking, political ideology, risk management, public consciousness, social scoring.*