


Научная статья  
УДК 34(341.217(4):004.8)  
DOI: 10.47475/2311-696X-2024-42-3-107-112

С. 107–112

## ЗАПРЕЩЕННЫЕ ДЕЙСТВИЯ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАКОНОДАТЕЛЬСТВЕ ЕВРОПЕЙСКОГО СОЮЗА

Артем Геннадьевич Шейкин

*Всероссийский государственный университет юстиции (РПА Минюста России) Москва, Россия*  
*sheykin.art@gmail.com*

 <https://orcid.org/0009-0000-3537-0202>

**Аннотация.** Статья посвящена исследованию норм закона Европейского союза об искусственном интеллекте в части неприемлемых рисков искусственного интеллекта. Обращается внимание на то, что основной идеей европейского подхода является поддержка развития заслуживающего доверия искусственного интеллекта, в связи с чем поставлен акцент на риск-ориентированный подход. Указывается, что неприемлемый риск является одним из уровней такого подхода, включающего также системы искусственного интеллекта с минимальным, ограниченным и высоким риском. Использование систем искусственного интеллекта неприемлемого риска относится к действиям, запрещенным законодательством Европейского союза, за исключением их применения в ряде обстоятельств, обозначенных в законе. Рассмотрены методы, воздействующие на подсознание; манипулятивные и вводящие в заблуждение методы; методы, использующие уязвимость человека или группы лиц; методы биометрической идентификации; прогностические методы, основанные на профилировании; методы определения эмоций. Проанализированы исключения, допускаемые законом в отношении систем искусственного интеллекта неприемлемого риска. Сделан вывод о том, что отсутствие в России широкого нормативно-правового регулирования искусственного интеллекта нельзя однозначно признать негативным фактором, так как законодатель имеет возможность проанализировать результаты правовых подходов к регулированию в зарубежных странах. Заключается, что в Российской Федерации отсутствует необходимость принятия закона, предметно посвященного искусственному интеллекту. Соответствующие нормы вполне могут быть имплементированы в действующее отраслевое законодательство.

**Ключевые слова:** искусственный интеллект, закон Европейского союза об искусственном интеллекте, правовое регулирование технологий искусственного интеллекта, сравнительное правоведение


**Для цитирования:** Шейкин А. Г. Запрещенные действия в области искусственного интеллекта в законодательстве Европейского союза // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 107–112. DOI: 10.47475/2311-696X-2024-42-3-107-112

Research article

## PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES IN THE LEGISLATION OF THE EUROPEAN UNION

Artem G. Sheikin

*All-Russian State University of Justice, Moscow, Russia*  
*sheykin.art@gmail.com*

 <https://orcid.org/0009-0000-3537-0202>

**Abstract.** The article is devoted to the study of the norms of the European Union law on Artificial Intelligence in terms of unacceptable risks of artificial intelligence. Attention is drawn to the fact that the main idea of the European approach is to support the development of trustworthy artificial intelligence, in connection with which the emphasis is placed on a risk-based approach. It is indicated that unacceptable risk is one of the levels of such an approach, which also includes artificial intelligence systems with minimal, limited and high risk. The use of unacceptable risk artificial intelligence systems refers to actions prohibited by the legislation of the European Union, except for their use in a number of circumstances specified in the law. Methods affecting the subconscious mind are considered; manipulative and misleading methods; methods using the vulnerability of a person or group of persons; methods of biometric identification; predictive methods based on profiling; methods for determining emotions. The exceptions allowed by law in relation to artificial intelligence systems of unacceptable risk are analyzed. It is concluded that the lack of broad regulatory regulation of artificial intelligence in Russia cannot be unequivocally recognized as a negative factor, since the legislator has the opportunity to analyze the results of legal

approaches to regulation in foreign countries. It is concluded that in the Russian Federation there is no need to adopt a law specifically devoted to artificial intelligence. The relevant norms may well be implemented in the current industry legislation.

**Keywords:** artificial intelligence, the law of the European Union on Artificial Intelligence, legal regulation of artificial intelligence technologies, comparative law

**For citation:** Sheikin AG. Prohibited Artificial Intelligence Practices in the Legislation of the European Union. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(3):107-112. (In Russ.) DOI: 10.47475/2311-696X-2024-42-3-107-112

## Введение

13 марта 2024 г. Европейским парламентом большинством голосов был одобрен Закон об искусственном интеллекте Европейского союза (EU AI Act, далее также — Закон ЕС об ИИ, Закон)<sup>1</sup>. Этот Закон является первым в мире нормативным правовым актом, всесторонне регламентирующим общественные отношения, возникающие по поводу создания, внедрения и использования технологий искусственного интеллекта (далее — ИИ).

Закон ЕС об ИИ является частью широкого пакета политических мер по поддержке развития ИИ, включающего «Инновационный пакет искусственного интеллекта» (AI Innovation Package)<sup>2</sup> и «Координационный план по искусственному интеллекту» (Coordinated Plan on AI)<sup>3</sup>. Вместе с тем его необходимо рассматривать и в контексте других законов о цифровизации, таких как Закон о цифровых услугах (Digital Services Act)<sup>4</sup> и Закон о цифровых рынках (Digital Markets Act)<sup>5</sup>, которые регулируют крупные коммерческие онлайн-платформы, такие как Google, Amazon, Meta<sup>6</sup> и Apple, а также в контексте Закона о цифровом управлении (Digital Governance Act)<sup>7</sup>. Несмотря на то, что крупные технологические гиганты активно используют ИИ, тем не менее, «они не являются объектом внимания Закона: вместо этого он в основном, хотя и не исключительно, нацелен на ИИ в государственном секторе и правоохранительных органах» [5, с. 6].

Основной идеей принятия Закона ЕС об ИИ обозначена поддержка развития *заслуживающего доверия* искусственного интеллекта, в связи с чем центральной темой регулирования европейского Закона является риск-ориентированный подход. В статье 3 Закона ЕС об ИИ понятие «риск» раскрывается как «сочетание вероятности причинения вреда и тяжести этого вреда».

15 февраля 2024 г. в Национальную стратегию развития искусственного интеллекта на период до 2030 года, утвержденную Указом Президента РФ от 10.10.2019 № 490, был введен раздел «Создание комплексной системы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта, обеспечение безопасности применения таких технологий». Риск-ориентированный подход заявлен как один из основных принципов нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта и, согласно Стратегии, подразумевает, что «уровень проработки, характер и детализация изменений при регулировании вопросов в области искусственного интеллекта должны соответствовать уровню рисков, создаваемых конкретными технологиями и системами искусственного интеллекта для интересов человека и общества»<sup>8</sup>.

В этой связи целесообразно рассмотреть подходы к законодательному регулированию этого направления в «первом Законе об искусственном интеллекте».

## Материалы и методы

В статье использованы теоретические источники и комментарии специалистов из различных областей права, посвященные вопросам правового регулирования ИИ, а также нормативные правовые акты международного и национального уровней по рассматриваемой проблематике. Основу исследования составили общенаучные и частнонаучные методы научного познания, анализ теоретических и нормативных правовых источников.

## Описание исследования

Нормативно-правовая база Закона ЕС об ИИ определяет четыре уровня риска для систем искусственного интеллекта: неприемлемый, высокий, ограниченный и минимальный. В рамках данной статьи рассмотрим категорию неприемлемого риска. Приложения ИИ считаются *неприемлемыми*, поскольку они «противоречат ценностям Союза, например, нарушая фундаментальные права» [5, с. 10]. Раздел II Закона ЕС об ИИ перечисляет их в ст. 5 под заголовком «Запрещенные действия в области искусственного интеллекта».

<sup>8</sup> О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом : Указ Президента Российской Федерации от 15 февраля 2024 г. № 124. URL: <http://www.kremlin.ru/acts/bank/50326> (дата обращения: 21.02.2024).

<sup>1</sup> URL: <https://artificialintelligenceact.eu/the-act/> (дата обращения: 14.03.2024).

<sup>2</sup> URL: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_383](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383) (дата обращения: 14.03.2024).

<sup>3</sup> URL: <https://digital-strategy.ec.europa.eu/en/policies/plan-ai> (дата обращения: 14.03.2024).

<sup>4</sup> URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065> (дата обращения: 14.03.2024).

<sup>5</sup> URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=0J%3AL%3A2022%3A265%3ATOC&uri=uriserv%3A0J.L\\_2022.265.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=0J%3AL%3A2022%3A265%3ATOC&uri=uriserv%3A0J.L_2022.265.01.0001.01.ENG) (дата обращения: 14.03.2024).

<sup>6</sup> Принадлежит компании Meta, **признанной экстремистской организацией, деятельность которой запрещена на территории РФ**.

<sup>7</sup> URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868> (дата обращения: 14.03.2024).

### Методы, воздействующие на подсознание, манипулятивные и вводящие в заблуждение методы

Пункт «а» ст. 5 Закона ЕС об ИИ запрещает размещение на рынке, ввод в эксплуатацию или использование системы ИИ, которая использует подсознательные техники за пределами сознания человека (*deploy subliminal techniques beyond a person's consciousness*) или целенаправленно манипулятивные или вводящие в заблуждение методы с целью существенного искажения поведения личности или группы лиц, которое существенно ухудшает способность человека принимать осознанное решение, тем самым заставляя лицо принять решение, которое в противном случае оно не приняло бы, следствием чего является причинение или возможность причинения значительного вреда этому лицу, другому лицу или группе лиц.

Манипулятивные методы с использованием ИИ могут оказать серьезное неблагоприятное воздействие на физическое, психическое здоровье или финансовые интересы. Такие системы ИИ используют аудио-, видеокомпоненты и изображения, которые люди не могут воспринимать, а даже если они осознают, что они обмануты, то не способны контролировать свое поведение или сопротивляться манипуляции<sup>1</sup>.

Этому могут способствовать, например, интерфейсы «машина-мозг» или виртуальная реальность: поскольку они обеспечивают более высокую степень контроля над тем, какие стимулы предъявляются людям, то могут существенно исказить их поведение. В частности, указывается, что «благодаря развитию новых технологий (например, электронного обоняния и осязания) и их креативной комбинации со связанными технологиями, включая... интерфейсы «мозг-компьютер», станет доступно гораздо больше манипулятивных подпороговых и надпороговых практик искусственного интеллекта» [7, с. 6]. Сюда же относится кумулятивный вред, который может накапливаться с течением времени [7, с. 7].

Запрещается также размещение на рынке, ввод в эксплуатацию или использование системы ИИ, которая использует любую уязвимость человека или группы людей из-за их возраста, инвалидности либо конкретной социальной или экономической ситуации, с целью последующего существенного искажения поведения этого лица или лица, относящегося к этой группе таким образом, что это причиняет или с достаточной вероятностью

<sup>1</sup> В качестве примеров в литературе приводится использование встроенных смайликов в видео гостиничных номеров, оказавшее значительное влияние на выбор потребителями отелей [6, с. 200] и других стимулов, воздействующих на подсознание, чтобы побуждать покупателей покупать больше продуктов (неэтичный маркетинг) [4, с. 1]. Стоит отметить, что согласно ст. 5 Закона РФ «О рекламе» не допускаются использование в радио-, теле-, видео-, аудио- и кинопродукции или в другой продукции и распространение скрытой рекламы, то есть рекламы, которая оказывает не осознаваемое потребителями рекламы воздействие на их сознание, в том числе такое воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами. Эта норма действует с момента принятия Закона в 2006 году // Российская газета. 2006. 15 марта.

может причинить этому лицу или другому лицу значительный вред (подп. «b» п. 1 ст. 5).

Намерение исказить поведение не может вменяться, если искажение является результатом внешних по отношению к системе ИИ факторов, находящихся вне контроля поставщика или развертывающего лица, то есть факторов, которые не могут быть разумно предвидены и смягчены. В любом случае поставщику или развертывающему лицу не обязательно иметь намерение причинить значительный вред, если такой вред является результатом манипулятивных или эксплуататорских практик с использованием ИИ. Запреты на такую практику ИИ дополняют положения, содержащиеся в Директиве 2005/29/ЕС<sup>2</sup>, в частности, недобросовестная коммерческая практика, ведущая к экономическому или финансовому ущербу для потребителей, запрещена при всех обстоятельствах, независимо от того, осуществляется ли она через системы ИИ или без таковых. Запреты манипулятивной и эксплуататорской практики в Законе ЕС об ИИ не затрагивают законную практику в контексте медицинского лечения, такую как лечение психических заболеваний или физическую реабилитацию, если такая практика осуществляется в соответствии с применимым законодательством и медицинскими стандартами, при наличии явного согласия отдельных лиц или их законных представителей. Кроме того, распространенная и законная коммерческая практика, например, в области рекламы, соответствующая применимому законодательству, сама по себе не должна рассматриваться как представляющая собой вредную манипулятивную практику ИИ.

### Методы биометрической идентификации

Запрещается размещение на рынке или ввод в эксплуатацию для этой конкретной цели или использование систем биометрической категоризации, которые *классифицируют* отдельных физических лиц на основе их биометрических данных, чтобы сделать заключение об их расе, политических взглядах, членстве в профсоюзе, религиозных или философских взглядах, убеждениях, сексуальной жизни или сексуальной ориентации (подп. «ba» п. 1 ст. 5).

Биометрические данные — это персональные данные, полученные в результате специальной технической обработки, связанной с физическими, физиологическими или поведенческими характеристиками физического лица, такие как изображения лица или дактилоскопические данные (п. 33 ст. 3).

Система биометрической категоризации подразумевает систему ИИ, предназначенную для отнесения физических лиц к определенным категориям на основе их биометрических данных, за исключением случаев, когда она является вспомогательной для другой коммерческой услуги и строго необходима по объективным техническим причинам (п. 35 ст. 3).

<sup>2</sup> URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029> (дата обращения: 14.03. 2024).



Система удаленной биометрической идентификации означает систему ИИ, предназначенную для идентификации физических лиц без их активного участия, как правило, на расстоянии, путем сравнения биометрических данных человека с биометрическими данными, содержащимися в справочной базе данных (п. 36 ст. 3). Запрещается использование систем удаленной биометрической идентификации «в реальном времени» в общедоступных местах в целях обеспечения правопорядка (подп. «ba» п. 1 ст. 5).

Закон различает систему удаленной биометрической идентификации «в режиме реального времени», в которой сбор биометрических данных, сравнение и идентификация происходят без значительной задержки (п. 37 ст. 3)<sup>1</sup>, и «пост-систему удаленной биометрической идентификации», отличную от системы удаленной биометрической идентификации «в реальном времени» (п. 38 ст. 3). Конкретным примером последней является крупномасштабная сеть видеонаблюдения, укомплектованная программным обеспечением для распознавания лиц [8, с. 101]. В этом контексте уместно также указать на запрет Закона ЕС об ИИ относительно размещения на рынке, ввода в эксплуатацию для этой конкретной цели или использования систем ИИ, которые создают или расширяют базы данных распознавания лиц посредством нецелевого извлечения изображений лиц из интернета или записей с камер видеонаблюдения (подп. «db» п. 1 ст. 5).

Запрет на использование систем удаленной биометрической идентификации «в реальном времени» в общедоступных местах не распространяется на случаи, когда это необходимо для одной из следующих целей, указанных в подп. «d» п. 1 ст. 5: (а) целенаправленный поиск конкретных жертв похищений, торговли людьми и сексуальной эксплуатации людей, а также поиск пропавших без вести лиц; (б) предотвращение конкретной, существенной и непосредственной угрозы жизни или физической безопасности физических лиц или реальной и настоящей или реальной и предсказуемой угрозы террористического нападения; (с) локализация или идентификация лица, подозреваемого в совершении уголовного преступления, в целях проведения уголовного расследования, судебного преследования или исполнения уголовного наказания за преступления, указанные в Приложении Па к Закону ЕС об ИИ и наказуемые в соответствующем государстве-члене ЕС лишением свободы или постановлением о заключении под стражу на срок не менее четырех лет<sup>2</sup>.

<sup>1</sup> Это включает в себя не только мгновенную идентификацию, но и ограниченные короткие задержки во избежание обхода.

<sup>2</sup> Список преступлений в Приложении Па включает: терроризм, торговлю людьми, сексуальную эксплуатацию детей и детскую порнографию, незаконный оборот наркотических средств и психотропных веществ, незаконный оборот оружия, боеприпасов и взрывчатых веществ, убийство, тяжкое телесное повреждение, незаконную торговлю человеческими органами и тканями, незаконный оборот ядерных или радиоактивных материалов, похищение людей, незаконное задержание и захват заложников, преступления, подпадающие под юрисдикцию Международного

При этом использование систем удаленной биометрической идентификации «в режиме реального времени» в общедоступных местах<sup>3</sup> для любой из целей, указанных в подп. «d» п. 1, должно применяться только для этих целей и для подтверждения личности конкретного лица должно учитывать следующие элементы (п. 2 ст. 5): (а) характер ситуации, приведшей к возможному использованию, в частности, серьезность, вероятность и масштаб вреда, причиненного в случае отсутствия использования системы; (б) последствия использования системы для прав и свобод всех заинтересованных лиц, в частности, серьезность, вероятность и масштаб этих последствий.

О каждом использовании системы удаленной биометрической идентификации «в режиме реального времени» в общедоступных местах в правоохранительных целях необходимо уведомлять соответствующий орган по надзору за рынком и национальный орган по защите данных в соответствии с национальными правилами (п. 3а ст. 5).

#### Методы формирования социального рейтинга

Запрещается размещение на рынке, ввод в эксплуатацию или использование систем ИИ для оценки или классификации физических лиц или их групп в течение определенного периода времени на основе их социального поведения или известных, предполагаемых или прогнозируемых личностных характеристиках в целях формирования социального рейтинга, приводящего к одному или двум последствиям: (а) вредное или неблагоприятное обращение с определенными физическими лицами или целыми их группами в социальных контекстах, не связанных с контекстами, в которых данные были первоначально созданы или собраны; (б) вредное или неблагоприятное обращение с определенными физическими лицами или их группами, которое является неоправданным или несоразмерным их социальному поведению или его серьезности (подп. «с» п. 1 ст. 5).

Система социального рейтинга, известная по ее широкому разветвлению в Китайской Народной Республике, получает неоднозначную оценку в российской и зарубежной литературе. Некоторые авторы видят в социальном рейтинге положительные составляющие [3], в то время как другие указывают на существенную разницу в менталитете европейцев и китайцев, вызывающую протест против встраивания человека в систему присвоения баллов [2]. Позиция Евросоюза, сформулированная в Законе ЕС об ИИ, четко демонстрирует эти

уголовного суда, незаконный захват самолетов/кораблей, изнасилование, экологические преступления, организованное или вооруженное ограбление, диверсию, участие в преступной организации, причастной к одному или нескольким преступлениям, перечисленным выше.

<sup>3</sup> «Общественно доступное пространство» означает любое физическое место, находящееся в государственной или частной собственности, доступное неопределенному числу физических лиц, независимо от того, могут ли применяться определенные условия доступа, и независимо от потенциальных ограничений вместимости (п. 39 ст. 3).

различия, категорически обозначая место систем социального рейтинга в разряде «неприемлемого риска».

#### **Прогностические методы, основанные на профилировании**

Запрещается размещение на рынке, ввод в эксплуатацию для этой конкретной цели или использование системы ИИ для оценки риска физических лиц с целью оценки или прогнозирования риска совершения физическим лицом уголовного преступления, основываясь исключительно на профилировании физического лица или оценке его личностных качеств и характеристик. Этот запрет не распространяется на системы ИИ, используемые для поддержки человеческой оценки участия человека в преступной деятельности, которая уже основана на объективных и поддающихся проверке фактах, непосредственно связанных с преступной деятельностью (подп. «da» п. 1 ст. 5). Применительно к расследованию преступлений профилирование представляет собой «методику составления портрета наиболее вероятного подозреваемого по расследуемому преступлению на базе информационных моделей, сформированных по результатам анализа отдельных элементов, следов и психологических особенностей ранее совершенных преступлений» [1, с. 12]. По смыслу Закона ЕС об ИИ «профилирование» означает любую форму автоматизированной обработки персональных данных, зафиксированную в соответствующих регламентах и директивах ЕС (п. 44be ст. 3).

#### **Методы определения эмоций**

Запрещается размещение на рынке, ввод в эксплуатацию для этой конкретной цели или использование систем ИИ для определения эмоций физического лица на рабочих местах и в учебных заведениях, за исключением случаев, когда использование системы ИИ используется по медицинским соображениям или соображениям безопасности (подп. «dc» п. 1 ст. 5). Система распознавания эмоций означает систему ИИ, предназначенную для идентификации либо определения эмоций или намерений физических лиц на основе их биометрических данных (п. 34 ст. 3).

#### **Санкции**

П. 3 ст. 71 предусматривает, что несоблюдение запрета на использование ИИ, упомянутого в ст. 5, влечет за собой административные штрафы в размере до 35 000 000 евро или, если правонарушителем является компания, до 7 % от ее общего мирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма окажется выше.

#### **Заключение и выводы**

Не подлежит сомнению, что Закон ЕС об ИИ как первый нормативный правовой акт, посвященный регулированию этой сферы общественных отношений, — это серьезный задел для разработки соответствующего законодательства других стран. Более того, отставание России в этом направлении нельзя однозначно признать негативным фактором, так как законодатель имеет возможность проанализировать последствия тех или иных подходов к регулированию в зарубежных странах.

Основной вопрос, возникающий при анализе законодательных новелл Евросоюза — это вопрос о необходимости разработки подобного, предметно посвященного ИИ федерального закона. Рассмотрев эту проблему пока только лишь через призму анализа «неприемлемых рисков», можно увидеть, что соответствующие нормы вполне могут быть имплементированы в действующее отраслевое законодательство. В первую очередь, речь идет о Законе РФ «Об информации, информационных технологиях и о защите информации», а также об Уголовно-процессуальном кодексе РФ, Трудовом кодексе РФ, Кодексе РФ об административных правонарушениях, Законе РФ «Об основах охраны здоровья граждан в Российской Федерации», Законе «Об оперативно-розыскной деятельности», «О полиции», «О рекламе», «О средствах массовой информации» и др.

Таким образом, «первый Закон об искусственном интеллекте» дает серьезный стимул к внесению в российское законодательство соответствующих изменений, направленных на формирование правовой базы, обеспечивающей высокие стандарты защиты прав человека и развитие заслуживающей доверия национальной системы искусственного интеллекта в рамках этих стандартов.

#### **Список источников**

1. Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. Москва : Проспект, 2021. 816 с.
2. Побережная О. Е., Притульчик Е. И. Социально-правовая защита личного пространства граждан и системы социального рейтинга // Конституционно-правовые основы развития Республики Беларусь как социального государства в современных условиях : материалы междунар. науч.-практ. конф. (Минск, 3–4 октября 2019 г.). Минск : Белорусский государственный университет, 2019. С. 246–251.
3. Гончаров В. В., Петренко Е. Г., Борисова А. А., Толмачёва Л. В., Дмитриева И. А. Система социального доверия (социального рейтинга) в КНР: проблемы и перспективы внедрения в Российской Федерации // Административное и муниципальное право. 2023. № 3. С. 78–91. DOI: 10.7256/2454-0595.2023.3.39983
4. Albarrak L., Metatla O., Roudaut A. Exploring the influence of subliminal stimulus type and peripheral angle on the priming effect // International Journal of Human — Computer Studies. 2021. Vol. 151. P. 1–17. DOI:10.1016/j.ijhcs.2021.102631
5. Edwards L. The EU AI Act: a summary of its significance and scope // Artificial Intelligence (the EU AI Act). 2021. Vol. 1. 25 p.

6. Hsu L., Chen Y.J. Neuromarketing, subliminal advertising, and hotel selection: An EEG study // Australasian Marketing Journal. 2020. Vol. 28, no. 4. P. 200–208.
7. Neuwirth R. J. Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA) // Computer Law & Security Review. 2023. Vol. 48. P. 1–20.
8. Veale M., Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach // Computer Law Review International. 2021. Vol. 22, no. 4. P. 97–112.

**КОНФЛИКТ ИНТЕРЕСОВ**

Конфликт интересов отсутствует.

**CONFLICT OF INTEREST**

There is no conflict of interest.

Дата поступления статьи / Received: 25.04.2024.

Дата рецензирования статьи / Revised: 10.06.2024.

Дата принятия статьи к публикации / Accepted: 15.07.2024.

---