

Искусственный интеллект как средство управления в условиях глобальных рисков

Карцхия А. А.*

Ключевые слова: субъекты права, цифровые технологии, цифровые права, риски и угрозы, интеллектуальная собственность, интеллектуальные права, риск-менеджмент.

Аннотация.

Цель статьи — обосновать необходимость опережающей разработки нормативно-правовой базы практического применения технологий искусственного интеллекта и регулирования имущественного оборота объектов, снабженных технологиями искусственного интеллекта.

Метод исследования — компаративный анализ современного состояния и правового регулирования технологий искусственного интеллекта, концептуальная оценка влияния и характеристика правовых рисков использования технологий искусственного интеллекта.

Результат: в статье проводится анализ особенностей искусственного интеллекта с точки зрения права и правовых рисков применения технологий искусственного интеллекта в условиях формирования новой технологической среды, рассматривается новая область имущественного гражданского оборота с использованием технологий искусственного интеллекта, цифровых активов, иных современных цифровых технологий (криптовалют и токенов, виртуального имущества, робототехнических устройств, цифровых двойников, больших данных, облачных компьютерных сервисов и др.). Оцениваются правовые риски при использовании искусственного интеллекта и их значение, включая систематизацию оснований, форм и пределов ответственности искусственного интеллекта, объем правосубъектности объектов с технологиями искусственного интеллекта, а также анализируется возможность формирования специальных норм законодательства по созданию и использованию искусственного интеллекта в рамках института интеллектуальной собственности и имущественного гражданского оборота. Автор обосновывает необходимость расширения законодательной базы для практического использования и применения технологий искусственного интеллекта, важность построения комплексной модели правового регулирования, включающей формирование универсальных стандартов и правил применения искусственного интеллекта в имущественном обороте.

DOI: 10.21681/2226-0692-2020-1-45-50

Современные цифровые технологии оказывают существенное влияние на развитие традиционных отраслей экономики и стали составной частью современных управленческих систем в сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Понимание искусственного интеллекта

Системы искусственного интеллекта, как отмечается в специальном докладе Всемирной организации интеллектуальной собственности (ВОИС)², становятся все более очевидным фактором важных прорывов в технологии и бизнесе: от беспилотных автомобилей до средств медицинской диагностики и применения новейших методов производства в промышленности. Техно-

логии искусственного интеллекта, распространение которых основано на массовом использовании цифровой информации и стремительном росте вычислительной мощности компьютеров, выходят из сферы чисто теоретических исследований и становятся одним из сегментов мирового рынка, что может иметь по-настоящему революционные последствия. Устанавливая связи между миллиардами внешне не связанных друг с другом элементов информации, системы искусственного интеллекта в состоянии обеспечивать повышение точности прогнозов погоды и рост урожайности культур, улучшать диагностику раковых заболеваний, предсказывать эпидемии и повышать производительность труда в промышленности.

Технологии искусственного интеллекта обычно группируются таким образом, чтобы отразить три разных аспекта:

➤ *методы*, применяемые при создании искусственного интеллекта (например, машинное обучение);

² Искусственный интеллект. Доклад ВОИС 2019 г. URL: <http://www.wipo.int>.

¹ Карцхия Александр Амиранович, кандидат юридических наук, профессор РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, Российская Федерация.
E-mail: arhz50@mail.ru

- › функциональные приложения (например, обработка речи и компьютерное зрение);
- › области применения этих технологий (например, связь или транспорт).

Наиболее распространенные области применения искусственного интеллекта показаны на рис. 1:

зрения выявления и устранения междисциплинарных «пробелов» регулирования для обеспечения безопасности, исключения неопределенности и риска автономных систем. Такая оценка может послужить основой для разработки более детальных моделей обеспечения безопасности и способствовать более эффективному контролю рисков. Наряду с макроэкономическими риска-

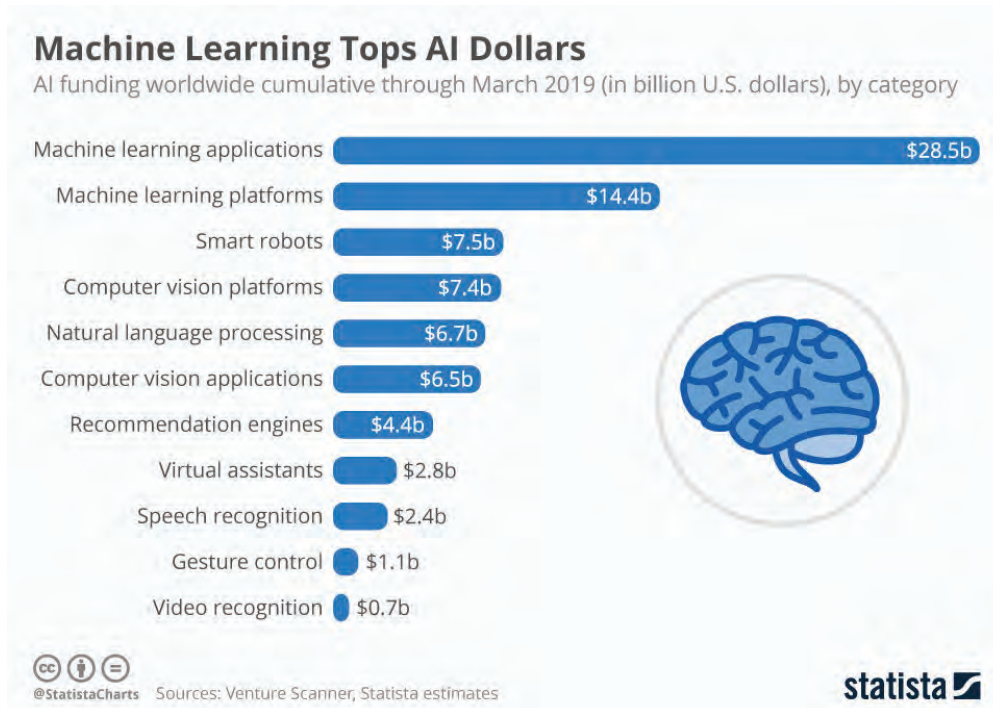


Рисунок 1

В свое время искусственный интеллект (ИИ), если не вдаваться в подробности научных дискуссий по этому вопросу [1, 2], получил обобщающее определение как технологии, которые стремятся воспроизвести или превзойти способности (с использованием вычислительных систем), которые потребовали бы «интеллекта», если бы люди должны были выполнять их³. К таким технологиям относятся: обучение и адаптация; сенсорное понимание и взаимодействие; рассуждение и планирование; оптимизация процедур и параметров; автономия и творчество. Новые подходы в отношении ИИ, разработанные в последнее десятилетие, и в частности, использование нейронных сетей глубокого обучения, значительно расширили возможности ИИ распознавать сложные паттерны, оптимизировать для конкретных результатов и принимать автоматизированные решения. Это требует обработки огромных объемов релевантных данных, разработки сильного алгоритма, определения направленной области и конкретной цели, что в совокупности может обеспечить значительное повышение надежности, эффективности и производительности ИИ.

Интересен взгляд на понимание сущности ИИ с позиции современных глобальных угроз и рисков. В частности, интересен подход ряда авторов [14] с точки

ми, геополитическими и геоэкономическими угрозами и напряженностью, экологическими и климатическими рисками, биологическими угрозами, как отмечалось на Всемирном экономическом форуме 2020⁴, в настоящее время глобальными признаются и технологические риски. Технологии продолжают играть важную роль в формировании глобального ландшафта рисков. Технологические угрозы связаны с мошенничеством в отношении персональных данных и кибератаками на них, что повлекло ужесточение законодательства о персональных данных в Европе и других странах мира, где был выявлен ряд технологических уязвимостей. Ожидается, что риски, связанные с фейковыми новостями и кражей личных данных, будут только увеличиваться. Это сопровождается также угрозами для конфиденциальности корпоративных и государственных данных и информации. Выявляемые массовые утечки данных, угрозы программному обеспечению показали потенциальное использование ИИ для разработки более мощных кибератак. Получены дополнительные доказательства того, что кибератаки создают риски для критически важной инфраструктуры, что побудило страны усилить контроль за трансграничными сделками и кооперацией по соображениям национальной безопасности.

³ Guidelines for AI Procurement. 2019 World Economic Forum. URL: <http://weforum.org>.

⁴ The Global Risks Report. 2019. World Economic Forum. URL: <http://weforum.org>.

Цифровые технологии оказывают существенное влияние на развитие традиционных отраслей экономики и стали составной частью современных управленческих систем в предпринимательстве, государственном управлении, в таких сферах как оборона страны, безопасность государства и обеспечение правопорядка, создают новые бизнес-модели [3—5].

ИИ в правовом регулировании рассматривается как новый вызов для правовой системы, новое явление, имеющее мультипликационный эффект, правовой феномен в структуре правоотношений, новый объект для правового регулирования.

Применимость и возможности искусственного интеллекта

ИИ все чаще становится движущей силой важных разработок в области технологий и бизнеса, от автономных транспортных средств до медицинской диагностики и передового производства. В наши дни ИИ стал объектом не только теоретических исследований, но вышел на глобальный рынок, его рост стимулируется обилием оцифрованных данных и быстро развивающимися вычислительными мощностями обработки таких данных⁵.

Важно заметить, что ИИ получил легальное определение в стратегических документах Российской Федерации. Так, в соответствии с утвержденной Президентом РФ Национальной стратегией развития искусственного интеллекта на период до 2030 года (далее — Национальная стратегия⁶) ИИ представляет собой комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (включая машинное обучение), процессы и сервисы по обработке данных и поиску решений. К разновидностям ИИ Национальная стратегия относит технологии, основанные на использовании ИИ, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта. Феномен ИИ проявляется в следующих факторах влияния:

➤ *способы использования ИИ*: продвинутые формы статистических и математических моделей (машинное обучение, нечеткая логика и экспертные системы), позволяющие решать задачи, обычно выполняемые людьми. Способы использования ИИ служат в качестве средства реализации различных функций ИИ.

➤ *функциональные возможности ИИ*: предиктивная аналитика, методы контроля, планирование и диспетчеризация, роботы, хранение, обработка и представление знаний и обоснований; распределенный ИИ; речь и компьютерное зрение; речевые функции (включая общую обработку речи, распознавание речи, фонология, синтез речи, речевой диалог, распознавание диктора), а также компьютерное зрение (включая дополненную реальность, биометрию, сегментацию изображений и видео, распознавание символов, слежение за объектом, понимание сцены, общее зрение); обработка естественного языка (включая извлечение информации, машинный перевод, диалог). Эти функции используются как самостоятельно, или могут быть реализованы в их совокупности.

Сферы применения ИИ: различные области (промышленность, транспорт, сельское хозяйство, медицина, образование, государственное управление и др.) или дисциплины, где способы ИИ или функциональные его приложения могут найти применение, включая аффективные вычисления, персональные компьютеры и приложения для ПК; Интернет вещей (IoT), компьютерные сети/Интернет; аэрокосмическая отрасль и авионика, автономные транспортные средства и управление ими; радиовещание и телевидение, все виды связи; обнаружение аномалий/наблюдение, идентификация, криптография и компьютерная безопасность; «умные» города и иные «умные» объекты; социальные связи; обслуживание клиентов и электронная коммерция; право, социальные и поведенческие науки.

Разновидности ИИ быстро осваиваются в ряде секторов, где возможно обнаружение закономерности в больших объемах данных и моделирование сложных, взаимозависимых системы для улучшения принятия решений изготвление и экономия затрат⁷, включая автономные транспортные средства, НИОКР с обработкой крупномасштабных данных, интеллектуальная медицина и здравоохранение, финансы и расчеты, маркетинг и реклама, сельское хозяйство; прогнозирование полицейской деятельности и оценки риска повторных правонарушений, прогнозирование законодательства и правоприменения, а также автоматизация обнаружения и реагирования на угрозы в режиме реального времени.

В то же время, ИИ с точки зрения способности участия в имущественном обороте представляет собой компьютерную систему, действующая на основе определенных принципов, которая может для заданного набора целей, определенных человеком, делать прогнозы, рекомендации или решения, влияющие на реальную или виртуальную среду, и предназначена для работы с различными уровнями автономности.

В этом смысле ИИ выступает как программно-аппаратный комплекс. К разновидностям ИИ относят:

➤ *слабый ИИ*, способный решать только узкоспециализированные задачи;

⁵ WIPO Technology Trends 2019: Artificial Intelligence. URL: <http://www.wipo.int>.

⁶ Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ, 14.10.2019, № 41, ст. 5700.

⁷ OECD Recommendation of the Council on Artificial Intelligence. OECD. 2019. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

› **универсальный (сильный) ИИ**, способный подобно человеку решать комплексные задачи, самостоятельно мыслить, взаимодействовать и адаптироваться к изменяющимся условиям, использовать большие данные.

ИИ стал инструментом правового регулирования, но, тем не менее, с точки зрения права он не обладает самостоятельной правосубъектностью и рассматривается как объект правового регулирования, т. е. имущество, подконтрольное физическому или юридическому лицу. При этом существует множество научных точек зрения в отношении правосубъектности ИИ [6—12].

В настоящей статье автор исходит из понимания ИИ как имущества, не обладающего самостоятельной правосубъектностью, т. е. как сложной, комплексной технологией, поскольку именно в таком виде ИИ преимущественно используется в сфере производственных экономических отношений.

Новые достижения в области ИИ обусловлены взаимодействием между информатикой и когнитивной наукой. Идея глубокой нейронной сети (используемой для применения ИИ в автономных транспортных средствах, создание новых лекарств и генетических объектов и др.) базируется на механизмах работы человеческого мозга, применении машинного обучения на базе множества вычислительных систем, организованных по принципу нейронных сетей.

ИИ рассматривается и как комплекс технологических решений, имитирующий когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и способный получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску решений, что позволяет рассматривать его в качестве объекта регулирования в сфере интеллектуальной собственности и возможности защиты интеллектуальных прав.

Искусственный интеллект в условиях глобальных рисков

Оценка масштабов и тенденций применения ИИ во многом связано с глобальными рисками и вызовами современности. Наряду с глобальными технологическими рисками, связанными с использованием современных цифровых технологий, включая искусственный интернет, с нашей точки зрения существуют и экономические риски использования ИИ. В Национальной стратегии (п. 16, 17) указано, что с учетом сложившейся обстановки на глобальном рынке ИИ и среднесрочных прогнозов его развития, реализация Национальной стратегии является необходимым условием вхождения Российской Федерации в группу мировых лидеров в области развития и внедрения технологий ИИ и, как следствие, технологической независимости и конкурентоспособности страны. При этом отмечается, что не-

многочисленные ведущие участники глобального рынка ИИ предпринимают активные действия для обеспечения своего доминирования на этом рынке и получения долгосрочных конкурентных преимуществ, создавая существенные барьеры для достижения другими участниками рынка конкурентоспособных позиций.

В Национальной стратегии определяется наряду с другими направлениями и экономическая направленность ИИ, исходя из того, что использование технологий искусственного интеллекта в отраслях экономики носит общий («сквозной») характер и способствует созданию условий для улучшения эффективности и формирования принципиально новых направлений деятельности хозяйствующих субъектов, в том числе за счет:

а) повышения эффективности процессов планирования, прогнозирования и принятия управленческих решений (включая прогнозирование отказов оборудования и его превентивное техническое обслуживание, оптимизацию планирования поставок, производственных процессов и принятия финансовых решений);

б) автоматизации рутинных (повторяющихся) производственных операций;

в) использования автономного интеллектуального оборудования и робототехнических комплексов, интеллектуальных систем управления логистикой;

г) повышения безопасности сотрудников при выполнении бизнес-процессов (включая прогнозирование рисков и неблагоприятных событий, снижение уровня непосредственного участия человека в процессах, связанных с повышенным риском для его жизни и здоровья);

д) повышения лояльности и удовлетворенности потребителей (в том числе направление им персонализированных предложений и рекомендаций, содержащих существенную информацию);

е) оптимизации процессов подбора и обучения кадров, составления оптимального графика работы сотрудников с учетом различных факторов.

В наши дни государства все чаще стремятся использовать возможности, предоставляемые искусственным интеллектом, для повышения производительности государственного сектора и предоставления услуг населению, а также для стимулирования экономики. Как указывается в рекомендациях Всемирного экономического форума⁸, ИИ обладает потенциалом для значительного улучшения деятельности государства и удовлетворения потребностей граждан новыми способами, начиная от управления дорожным движением и заканчивая предоставлением медицинских услуг и обработкой налоговых форм. Однако правительствам зачастую не хватает опыта в приобретении современных решений в области ИИ, и многие государственные учреждения с осторожностью относятся к использованию этой мощной технологии. В частности, это относится к сфере государственных закупок, что определяют следующие подходы [13].

Во-первых, риски предвзятости, нарушения конфиденциальности и подотчетности и, в целом, прозрачности в этой сфере достаточно велики. Возникают не-

⁸ Guidelines for AI Procurement. 2019 World Economic Forum. URL: <http://weforum.org>.

вые инциденты, связанные с негативными последствиями использования искусственного интеллекта также и в таких областях, как вынесение уголовных приговоров, правоохранительная деятельность и даже сфера трудоустройства. Инновационные подходы в этих и других областях, с точки зрения рационального применения искусственного интеллекта, могут предотвратить возможные негативные последствия.

В-вторых, как уже отмечалось, в последние годы ИИ стремительно развивается, стимулируя дальнейшие исследования и прикладные разработки. Новые, представляющие интерес виды использования ИИ будут по-прежнему появляться и приносить с собой как выгоды, так и риски.

Наконец, правила и практика государственных закупок часто оказывают сильное влияние на рынки, особенно на ранних стадиях их развития, что обуславливает установление специальных стандартов применения технологий ИИ.

Расширение применения технологий искусственного интеллекта

ИИ стал инструментом правового регулирования, но, тем не менее, с точки зрения современного права он не обладает самостоятельной правосубъектностью и рассматривается как объект правового регулирования, т. е. имущество, подконтрольное физическому или юридическому лицу.

Используемый в современном праве режим правовой охраны ИИ только с позиций защиты интеллектуальных прав (прав интеллектуальной собственности) на компьютерные программы (их комплекс) явно не достаточен. Правовые дискуссии о возможности защиты прав ИИ на создаваемые им самостоятельно произведения в сфере авторского права лишь частично решают вопросы использования технологий ИИ и в полной мере не отвечают перспективным возможностям их применения, что создает препятствия к расширению внедрения таких технологий.

Новые достижения в области ИИ вызваны взаимодействием информатики и когнитивной наукой. Идея глубокой нейронной сети (используемой для применения искусственного интеллекта в автономных транспортных средствах, создании новых лекарств и генетических объектов и др.) базируется на механизмах работы человеческого мозга, применении машинного обучения на базе множества вычислительных систем, организованных по принципу нейронных сетей.

ИИ рассматривается и как комплекс технологических решений, имитирующий когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и способный получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску

решений, что позволяет рассматривать его в качестве объекта регулирования в сфере интеллектуальной собственности и возможности защиты интеллектуальных прав.

Безопасность как один из основных принципов использования ИИ заключается в недопустимости использования ИИ в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий ИИ, как отмечается в Национальной стратегии развития искусственного интеллекта.

Это предполагает, в том числе, прогнозирование рисков и неблагоприятных событий, снижение уровня непосредственного участия человека в процессах, связанных с повышенным риском для его жизни и здоровья. Таким образом, ИИ становится фактором информационной безопасности.

Оценка риска, в соответствии с ГОСТ РФ, включает в себя процесс идентификации внутренних и внешних угроз уязвимостей, идентификацию вероятности опасного события, возникшего при реализации этих угроз или уязвимостей, определение критических видов деятельности, для которых необходимо обеспечение бесперебойной работы, определение средств управления на местах, необходимых для снижения распространения последствий опасного события, и оценка стоимости таких средств управления.

Участие в имущественном обороте предполагает у его участников навыки идентификации угроз и опасностей, оценку риска, уязвимостей и опасностей, анализ воздействий на деятельность. В этом смысле ИИ может найти широкое применение, включая разработку различных бизнес-моделей предпринимательской деятельности, в том числе и в виртуальном мире сети Интернет.

Развитие внедрения искусственного интеллекта связано с разработкой:

- ▶ (а) стандартов и эталонов безопасности функционирования ИИ;
- ▶ (б) комплексной системы безопасности использования технологий ИИ;
- ▶ (в) этических правил взаимодействия человека с ИИ.

Отсюда необходимость выявления и систематизация рисков при использовании ИИ, включая правовые аспекты таких рисков, к которым можно отнести основания, формы и пределы ответственности ИИ, объем правосубъектности для каждой технологии ИИ, формирование специальных норм законодательства по созданию и использованию ИИ в рамках института интеллектуальной собственности и имущественного гражданского оборота, создание эталонной классификации технологий ИИ для определения режима правовой охраны и способов использования ИИ в имущественном обороте для каждой группы классификатора.

В качестве вывода. Расширение использования ИИ в гражданском обороте, в коммерческих отношениях и предпринимательской деятельности формирует запрос на создание специальных правовых норм, регулирующих сферу использования технологий ИИ, включая

нормы, определяющие правосубъектность и режимы правовой охраны, использования и защиты технологий ИИ, формы и виды ответственности при использовании технологий ИИ, создание эталонной классификации технологий ИИ.

Объективно необходима не только законодательная база для практического использования и применения технологий ИИ, но и построение комплексной мо-

дели правового регулирования, включающей в том числе формирование универсальных стандартов и правил применения ИИ в имущественном обороте и цифровой виртуальной технологической среде, регулирование способов и форм применения технологий ИИ, использования имущественных прав на технологии ИИ, особенностей правовых режимов регулирования в зависимости от вида технологии ИИ.

Литература

1. Нагродская В.Б. Новые технологии (блокчейн / искусственный интеллект) на службе права : научно-методическое пособие / под ред. Л.А. Новоселовой. М. : Проспект, 2019. 128 с.
2. Морхат П.М. Искусственный интеллект: правовой взгляд. М. : Буки Веди, 2017. 257 с.
3. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23. DOI: 10.21681/2311-3456-2019-2-18-23.
4. Карцхия А.А. Цифровые технологии в процессе «цифровой» адаптации права // ИС. Промышленная собственность. 2019. № 5. С.41—48.
5. Карцхия А.А. Цифровые технологические (онлайн) платформы: российский и зарубежный опыт регулирования // Гражданское право. 2019. № 3. С. 25—28. DOI: 10.18572/2070-2140-2019-3-25-28.
6. Юридическая концепция роботизации : монография / Н.В. Антонова, С.Б. Бальхаева, Ж.А. Гаунова и др.; отв. ред. Ю.А. Тихомиров, С.Б. Нанба. М. : Проспект, 2019. 240 с.
7. Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / В.В.Архипов, В.В.Бакуменко, А.Д.Вольнец и др. / под ред. А.В.Незнамова. М. : Инфотропик Медиа, 2018. 232 с.
8. Витко В. Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // ИС. Авторское право и смежные права. 2019. № 2. С. 5—20. № 3. С. 5—22.
9. Попова Н.Ф. Основные направления развития правового регулирования использования искусственного интеллекта, роботов и объектов робототехники в сфере гражданских правоотношений // Современное право. 2019. № 10. С. 69—73. DOI: 10.25799/NI.2019.30.55.003.
10. Дурнева П.Н. Искусственный интеллект: анализ с точки зрения классической теории правосубъектности // Гражданское право. 2019. № 5. С. 3—33. DOI: 10.18572/2070-2140-2019-5-30-33.
11. Yuval Noah Harari. Homo Deus: A Brief History of Tomorrow. New York Times, 2018. 400 p.
12. Ray Kurzweil. The Singularity Is Near: When Humans Transcend Biology. Penguin Books. 2005.
13. Шмелева М.В. Цифровые технологии в государственных и муниципальных закупках: будущее или реальность // Актуальные проблемы российского права. 2019. № 12. С. 36—42. DOI: 10.17803/1994-1471.2019.109.12.036-042.
14. S. Burton, I. Habli, T. Lawton, J. McDermid, F. Morgan, Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective. Elsevier, Artificial Intelligence, Volume 279, February 2020. URL: <https://doi.org/10.1016/j.artint.2019.103201> .

Рецензент: Рожнов Сергей Николаевич, доктор юридических наук, профессор, заведующий кафедрой теории и истории государства и права, декан юридического факультета РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва, Россия.

E-mail: kafedra_tigr@mail.ru

