

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.168.55 EDN: EOPHCR

КЛАССИФИКАЦИЯ РИСКОВ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Научная статья

Баленко Е.Г.[1, *]

[1] ORCID : 0000-0002-4046-1317;

[1] Донской государственный аграрный университет, Персиановский, Российская Федерация

* Корреспондирующий автор (stability333[at]yandex.ru)

Предложена: 05.07.2025; Принята: 09.04.2026; Опубликована: 17.06.2026

Аннотация

Публикация посвящена вопросам информационной безопасности в контексте развития технологий искусственного интеллекта и обработки больших данных. Рассмотрены современные тенденции и приоритеты применения данных технологий, выявлены потенциальные угрозы и риски, связанные с их внедрением. Особое внимание уделено проблемам конфиденциальности данных, уязвимостям систем искусственного интеллекта и возможностям применения деструктивных программных воздействий. Автор предлагает конкретные рекомендации по повышению уровня информационной безопасности, созданию нормативной правовой базы и по совершенствованию использования технологий обработки больших данных и развития искусственного интеллекта. Также предложены основные направления по формированию концепции безопасной эксплуатации рассматриваемых технологий.

Ключевые слова: искусственный интеллект, большие данные, информационная безопасность, деструктивные программные воздействия, уязвимость системы.

CLASSIFICATION OF RISKS AND METHODS FOR COUNTERING THREATS POSED BY ARTIFICIAL INTELLIGENCE IN BIG DATA PROCESSING SYSTEMS

Research article

Balenko E.G.[1, *]

[1] ORCID : 0000-0002-4046-1317;

[1] Don State Agrarian University, Persianovsky, Russian Federation

* Corresponding author (stability333[at]yandex.ru)

Suggested: 05.07.2025; Accepted: 09.04.2026; Published: 17.06.2026

Abstract

The article is devoted to information security issues in the context of the development of artificial intelligence technologies and big data processing. Current trends and priorities of application of these technologies are considered, potential threats and risks associated with their implementation are identified. Particular attention is paid to data privacy issues, vulnerabilities of artificial intelligence systems and the possibilities of using destructive software influences. The author offers specific recommendations to improve information security, create a regulatory framework and improve the use of big data processing technologies and the development of artificial intelligence. The main directions for the development of the concept of safe operation of the technologies under consideration are also proposed.

Keywords: artificial intelligence, big data, information security, destructive software impacts, system vulnerability.

Введение

Современный этап развития информационно-телекоммуникационной инфраструктуры сопровождается резким ростом объёма информации, поступающей от различных систем сбора и обработки данных, сенсорных систем, а также социальных сетей. Совокупность указанных данных является «большими данными» и открывает уникальные возможности для улучшения качества решения задач в различных секторах экономики, системах управления, а также в области обеспечения безопасности граждан. Однако рассматриваемые возможности имеют высокую вероятность реализации только при наличии соответствующих технологий обработки данных, обеспечивающих решение специфических прикладных задач с определённым гарантированным качеством. В существующих условиях ведущие государства мира рассматривают технологии искусственного интеллекта как один из ключевых факторов достижения способности влияния на решения и действия в сфере государственной политики, управления и организации общества [1], [3].

Актуальность. В последние десятилетия фаза эволюции информационных и телекоммуникационных систем отмечена стремительным увеличением объемов разнообразной информации. Как отмечают авторы в публикациях [1], [3], [13], именно «большие данные» становятся ключевым ресурсом для принятия решений в экономике, управлении и безопасности. Однако, согласно работам [14], [15], потенциал больших данных реализуется лишь при наличии адекватных технологий обработки, среди которых ведущая роль отводится искусственному интеллекту.

В зарубежной литературе активно исследуются риски внедрения ИИ: этические аспекты [16], уязвимости нейросетей к потере управляемости, целостности и утечке конфиденциальной информации [15], [17]. В российской науке вопросы регулирования ИИ рассматриваются в работах [18], [19], однако комплексный анализ рисков именно с позиции национальной безопасности и правовой стабильности представлен фрагментарно. Большинство исследований фокусируются либо на технических, либо на правовых аспектах изолированно, что создаёт пробел в системном видении существующих угроз.

Проблема и обоснование исследования. Отсутствие единой методологии оценки и противодействия рискам ИИ (от манипуляции данными до возникновения «цифровой власти») снижает эффективность внедрения ИИ в России и создаёт угрозы национальной безопасности, указанные в Указе Президента № 490 от 10.10.2019 г. «О развитии искусственного интеллекта» [1]. Это определяет необходимость систематизации рисков и выработки практических мер реагирования.

Цель работы заключается в систематизации рисков применения технологий искусственного интеллекта в контексте обработки больших данных и разработке комплекса организационно-технических мер для их минимизации в российском правовом поле.

Задачи исследования:

1) провести анализ актуальных рисков внедрения систем ИИ, включая технические, социальные и правовые аспекты;

2) классифицировать выявленные угрозы по источникам возникновения и потенциальному ущербу;

3) сформулировать предложения по созданию контролируемой инфраструктуры ИИ (верифицированные модели, дата-центры, средства подавления деструктивных действий);

4) определить направления правового регулирования для снижения рисков параллельной цифровой власти и вмешательства в частную жизнь.

Классификация рисков и методы противодействия угрозам искусственного интеллекта в системах обработки больших данных

Страны за рубежом стремятся занять лидирующие позиции в области искусственного интеллекта (далее — ИИ). Именно системы ИИ должны лечь в основу создания инновационных технологий, которые приведут к прорывам в таких сферах, как экономика, аграрный сектор, здравоохранение и развитие умных городов [1], [2]. Под искусственным интеллектом понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в т.ч. в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиск решений [1], [5]. В России развитие искусственного интеллекта направлено на достижение ключевых целей: повышение уровня жизни и благосостояния граждан, усиление национальной безопасности и правовой стабильности, а также создание конкурентоспособной экономики, особенно в сфере ИИ, для того чтобы занять лидирующие позиции в мировом масштабе [1], [9], [10]. В рамках развития искусственного интеллекта в России выделяются следующие ключевые задачи [1], [2]:

– содействие научным исследованиям, направленным на ускоренное развитие искусственного интеллекта;

– разработка и оптимизация программных продуктов с применением ИИ-технологий;

– увеличение объема и улучшение характеристик данных, необходимых для развития технологий искусственного интеллекта;

– обеспечение наличия необходимого оборудования для реализации задач в области ИИ;

– развитие компетенций специалистов для удовлетворения потребностей российского рынка искусственного интеллекта и распространение информации о возможностях использования этих технологий среди населения.

Среди ключевых областей применения искусственного интеллекта в разных отраслях выделяются [1], [4], [12]:

– совершенствование результативности планирования, прогнозирования и принятия управленческих решений;

– внедрение автоматизации для стандартных производственных операций;

– активное использование автономных интеллектуальных систем, роботизированных решений и систем управления цепочками поставок;

– гарантия безопасности персонала в ходе выполнения рабочих задач;

– рост уровня лояльности и удовлетворенности потребителей;

– улучшение процедур найма и подготовки кадров, включая формирование оптимальных графиков работы с учетом различных аспектов.

В контексте социальной области, ключевыми векторами внедрения искусственного интеллекта выступают [1], [3], [9]:

– совершенствование уровня медицинского обслуживания, включая, например, проведение профилактических осмотров, диагностирование с использованием анализа изображений и предсказание возникновения болезней;

– повышение стандарта образовательных услуг, достигаемое путем адаптации учебной программы к индивидуальным нуждам учащихся и актуальным требованиям рынка труда;

– оптимизация государственных и муниципальных услуг, направленная на повышение их качества и одновременное уменьшение затрат на их обеспечение.

При этом существуют определенные риски, связанные с использованием технологий искусственного интеллекта, а именно:

1. Вынужденное заимствование иностранных технологий в области искусственного интеллекта в части использования программного и аппаратного обеспечения. Большая часть вычислений для искусственного интеллекта

производится посредством использования графических карт (в основном иностранных). Большинство платформ, на которых базируются системы искусственного интеллекта иностранные. Программное обеспечение указанных платформ может иметь недекларируемые возможности, программные закладки и недокументированные функции. Системы искусственного интеллекта могут предоставлять для использования несовременные разработки, которые могут допустить ошибки, иметь устаревшие функции, упрощённые открытые версии. Удалённый доступ к системам искусственного интеллекта находится у иностранного производителя, что может привести к утечке конфиденциальных данных и персональных данных [7], [8], [12].

2. Отсутствие необходимого и достаточного количества кадров. Увеличился рост потребности аналитиков, работающих с большими данными. В настоящее время количество вузов, где могут преподавать порядок работы с большими данными, ограничено. Соответственно возникает необходимость дополнительной подготовки преподавателей и ученых в области технологий искусственного интеллекта [1], [9].

3. Отсутствие адекватных средств контроля систем искусственного интеллекта. Не существует технических средств контроля работы системы искусственного интеллекта, что позволяет разработчику вносить недокументированные функции и недекларируемые возможности. Сформированная нейросеть — это совокупность настроенных элементов обработки, не содержащая сведений об использованных для обучения данных, а также о типах объектов и методах, которым система была обучена для их идентификации. Ручная проверка миллионов вычислений в нейронной сети невозможна. Даже небольшая доля неточностей, выявленная в тестовых проектах с применением искусственного интеллекта, может привести к существенным убыткам при масштабировании и использовании на больших массивах информации [5], [6], [10].

4. Возможность манипулирования системами искусственного интеллекта посредством воздействия и намеренного внесения изменений в данные систем искусственного интеллекта. Возможно целенаправленное искажение данных, взлом алгоритмов, манипулирование оперативной разработкой [7], [9], [12].

5. Введение в заблуждение систем искусственного интеллекта при помощи самих систем искусственного интеллекта. Возможна ложная подмена информации систем биометрической идентификации пользователя с помощью специальных систем генерации образов, доступных на открытом рынке. Также возможно осуществить подделку разметки для беспилотных автомобилей [9], [10], [11].

6. Создание иллюзорной реальности с целью использования не по назначению. Подделка голоса, изображений и видео, которые невозможно отличить от настоящих [8], [10].

7. Манипулирование общественным мнением и усиление интенсивности информационных войн за счет появления более совершенных генеративных и самообучающихся моделей. Цифровые платформы знают предпочтения и привычки пользователя и предлагают требуемую повестку, такую как неотразимая реклама, убедительная политическая пропаганда [8], [10].

8. Возникновение параллельной цифровой власти. Формируется новый класс цифровой власти. Это владельцы, разработчики, операторы, администраторы систем искусственного интеллекта и баз данных. Они получают власть по факту доступа к данным [7], [10].

9. Вмешательство в частную жизнь. Распознавание лиц и анализ данных о человеке из разных источников нарушают права человека на тайну личной жизни. Большинство данных, получаемых системами искусственного интеллекта не урегулированы в законодательстве [7], [8].

10. Риск роста социальной напряженности. За счёт потери миллионов рабочих мест и распространения работ, требующих более высокой квалификации может быть увеличено количество недовольных граждан [9], [10], [11].

11. Правовые риски с определением правового статуса самого искусственного интеллекта. Нет четкого правого определения по ответственности применения технологий и систем искусственного интеллекта при принятии решений, а именно привлечение ИИ или его разработчиков к ответственности за нарушение законодательства страны. Отсутствуют нормы права по наделению ИИ правами и обязанностями. Нет четкого понимания к какому статусу отнести ИИ, юридическое лицо, интеллектуальная собственность, либо другая форма [9], [10], [11].

Регулирование правовых аспектов использования систем искусственного интеллекта становится важнейшей задачей современного общества. Необходим комплексный системный подход, включающий разработку законодательных норм, создание специализированных судов и институтов контроля, чтобы обеспечить справедливое распределение ответственности и защиту прав всех участников правоотношений. В целях адекватного противодействия рискам при применении технологий обработки больших данных и развития ИИ предлагаем:

– привлечение инвестиций в направлении развития искусственного интеллекта, в частности в высокорискованное направление научно-исследовательских работ;

– формирование и применение технологий, а также методологической базы, для борьбы с информационными деструктивными воздействиями;

– создание единых контролируемых облачных решений сервисов искусственного интеллекта;

– обеспечение требуемого уровня защищенности данных для обучения нейронных сетей и для использования;

– создание и развитие единой базы верифицированных моделей и дата центров, предусматривающих достоверную поставку данных;

– упреждающая разработка средств подавления деструктивных действий искусственного интеллекта;

– обеспечение контроля и возможности расследования публичной утечки данных.

Полученные результаты и их новизна

Систематизировано 11 классов рисков применения ИИ, объединённых в три группы: *технологические* (заимствование иностранных решений, отсутствие средств контроля, манипуляция данными), *социально-правовые*

(цифровая власть, вмешательство в частную жизнь, рост напряжённости) и *операционные* (подделка образов, иллюзорная реальность, манипуляция обществом).

Выявлен новый класс угрозы: «параллельная цифровая власть» (владельцы систем ИИ получают влияние, не предусмотренное законодательством).

Предложен комплекс из 7 мер, включающий создание единых контролируемых облачных решений; формирование базы верифицированных моделей, упреждающую разработку средств подавления деструктивных действий ИИ и обеспечение возможности проведения тщательного анализа и проверки операций, транзакций или процессов утечек данных.

Научная новизна и оригинальность:

Впервые предложена трёхуровневая классификация рисков ИИ (технологический, социально-правовой, операционный) применительно к российской стратегии развития ИИ. В отличие от работ [15], [16], [17], [19], новизна состоит в выделении взаимосвязи между отсутствием средств контроля искусственного интеллекта и возникновением «недекларируемых возможностей» — аспект, ранее не рассматривавшийся комплексно. Оригинальность предложенных мер заключается в приоритете упреждающего подавления (а не только обнаружения) деструктивных действий ИИ, что отличает подход от стандартных моделей кибербезопасности.

Впервые сформулировано требование к возможностям проведения тщательного анализа и проверки операций, транзакций или процессов публичных утечек данных как самостоятельной мере, что не фигурирует в действующих редакциях нормативных правовых актов.

Заключение

В настоящее время в целях обеспечения защищенности от указанных угроз компании Европейского союза закладывают в регламентах информационно-технического взаимодействия и обмена данными юридические основы по раскрытию информации о сведениях, используемых для обучения моделей искусственного интеллекта. При этом юридические лица, выпускающие подобные модели, обязуют посредством применения комплексной системы штрафов публиковать сводку данных, использованных для обучения, архитектуру и принципы работы систем, а также документировать меры по обеспечению информационной безопасности.

В связи с вышеизложенным выделяем несколько направлений для будущих исследований, которые могут расширить возможности безопасного использования ИИ и повысить уровень защищенности данных, циркулируемых в моделях искусственного интеллекта:

– повышение уровня полноты и качества данных, используемых для обучения моделей ИИ;

– разработка комплексных решений с элементами ИИ для защиты от деструктивных программных воздействий и оперативного реагирования на угрозы безопасности;

– совершенствование существующих норм права в части, касающейся повышения уровня защищенности данных и метаданных.

Таким образом, необходимо уточнение существующих подходов к решению проблем, связанных с развитием и внедрением технологий искусственного интеллекта и обработки больших данных, на всех уровнях государства с реализацией соответствующих мер научно-методического характера.

Конфликт интересов

Не указан.

Рецензия

Мангушева А.Р., Казанский национальный исследовательский технологический университет, Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.168.55.1

Conflict of Interest

None declared.

Review

Mangusheva A.R., Kazan National Research Technological University, Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.168.55.1

Список литературы / References

1. Российская Федерация. Национальная стратегия развития искусственного интеллект на период до 2030 года : Указ Президента РФ : [принят Президентом Российской Федерации 2019-10-10]. 2019. — 40 с. — URL: https://base.garant.ru/72838946/. (дата обращения: 05.07.25).

2. Российская Федерация. Федеральный закон от 31.07.2020 г. No 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» : Федеральный закон №258-ФЗ : [принят Государственной Думой Федерального Собрания Российской Федерации 2020-07-22 : одобр. Советом Федерации Федерального Собрания Российской Федерации 2020-07-24]. 2020. — 48 с. — URL: http://www.kremlin.ru/acts/bank/45796. (дата обращения: 05.07.25).

3. Российская Федерация. Федеральный закон от 02.07.2021 No 331-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» : Федеральный закон №331-ФЗ : [принят Государственной Думой Федерального Собрания Российской Федерации 2021-06-16 : одобр. Советом Федерации Федерального Собрания Российской Федерации 2021-06-23]. 2021. — 44 с. — URL: http://publication.pravo.gov.ru/Document/View/0001202107020046. (дата обращения: 05.07.25).

4. ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллекта. — Введ. 2020-12-23. — Москва: Стандартинформ, 2021. — 16 С.

5. ГОСТ Р 59898-2021. Оценка качества систем искусственного интеллекта. Общие положения. — Введ. 2021-11-26. — Москва: Российский институт стандартизации, 2021. — 24 С.

6. ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения. — Введ. 2020-12-23. — Москва: Стандартинформ, 2021. — 16 С.

7. ГОСТ Р 59926-2021 Информационные технологии. Эталонная архитектура больших данных. Часть 2. Варианты использования и производные требования. — Введ. 2022-03-01. — Москва: Стандартинформ, 2022. — 294 С.

8. ГОСТ Р 70466-2022/ISO/IEC TR 205471:2020 Информационные технологии. Эталонная архитектура больших данных. Часть 1. Структура и процесс применения (ISO/IEC TR 20547-1:2020). — Введ. 2022-11-08. — Москва: Российский институт стандартизации, 2022. — 20 С.

9. Российская Федерация. Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект» на период 2021–2024 годы : Постановление Правительства России 2020. — URL: https://www.economy.gov.ru/material/file/28a4b183b4aee34051e85ddb3da87625/20201222.pdf. (дата обращения: 05.07.25).

10. ПНСТ 776-2022 Информационные технологии. Интеллект искусственный. Управление рисками. — Введ. 2022-11-02. — Москва: Российский институт стандартизации, 2022. — 28 С.

11. Самойлов А.В. Технологии искусственного интеллекта: возможности или угрозы / А.В. Самойлов // Журнал высоких гуманитарных технологий. — 2023. — 3. — С. 67–71. — URL: https://hi-hume.ru/files/files/HHJ_2023_03(3).pdf (дата обращения: 26.02.26).

12. Гибадуллин Р.Ф. Анализ параметров промышленных сетей с применением нейросетевой обработки / Р.Ф. Гибадуллин, Д.В. Лекомцев, М.Ю. Перухин // Искусственный интеллект и принятие решений. — 2020. — 1. — С. 80–87. — URL: http://www.isa.ru/aidt/2020-01/80_87.pdf (дата обращения: 11.08.25). — DOI: 10.14357/20718594200108

13. Manyika J. Big Data: The Next Frontier for Innovation, Comptetition, and Productivity / J. Manyika, B. Brown, J. Bughin et al. // Discover scientific knowledge and stay connected to the world of science; — 2011: Discover scientific knowledge and stay connected to the world of science, 2011. — URL: https://www.researchgate.net/publication/260480165_Big_Data_The_Next_Frontier_for_Innovation_Comptetition_and_Productivity. (accessed: 31.03.26).

14. Russell S.J. Artificial Intelligence: A Modern Approach (4th ed.). Pearson. / S.J. Russell, P. Norvig. — 2021: SPi Global, 2021. — 117 p. — URL: https://clck.ru/3UD6ke. (accessed: 25.03.26).

15. Goodfellow I Deep Learning (Adaptive Computation and Machine Learning series) / I Goodfellow, Y Bengio, A Courville. — 2016: Amazon, 2016. — 781 c. — URL: https://www.deeplearningbook.org/. (дата обращения: 31.03.26).

16. Floridi L. The Ethics of Artificial Intelligence / L. Floridi. — Oxford: University press, 2019. — 28 p. — URL: https://clck.ru/3UD6av. (accessed: 26.02.26).

17. Szegedy C Intriguing properties of neural networks / C Szegedy, W Zaremba, I Sutskever et al. // Cornelll University; — 2014: Cornell University, 2014. — URL: https://arxiv.org/abs/1312.6199. (accessed: 31.03.26).

18. Понкин И.В. Машиночитаемое право, цифровые модели-двойники, цифровая формализация и цифровая онто-инженерия в праве / И.В. Понкин, А.И. Лаптева. — Москва: Консорциум «Аналитика. Право. Цифра», 2021. — 174 с. — URL: https://clck.ru/3UD6fX. (дата обращения: 26.02.26).

19. Незнамов А Реакция отрасли: что ожидается от нового российского регулирования ИИ / А Незнамов. // ICT.Moscow; — Москва: ICT.Moscow, 2025.

Список литературы на английском языке / References in English

1. Russian Federation. Nacional'naya strategiya razvitiya iskusstvennogo intellekt na period do 2030 goda [National Strategy for the Development of Artificial Intelligence for the Period up to 2030] : Decree of the President of the Russian Federation : [accepted by President of the Russian Federation 2019-10-10]. 2019. — 40 p. — URL: https://base.garant.ru/72838946/. (accessed: 05.07.25). [in Russian]

2. Russian Federation. Federal'ny'j zakon ot 31.07.2020 g. No 258-FZ «Ob e'ksperimental'ny'x pravovy'x rezhimax v sfere cifrovy'x innovacij v Rossijskoj Federacii» [Federal Law No. 31.07.2020 dated 258-FZ "On Experimental Legal Regimes in the Field of Digital Innovations in the Russian Federation"] : Federal Law №258-ФЗ : [accepted by State Duma of the Federal Assembly of the Russian Federation 2020-07-22 : approved by Federation Council of the Federal Assembly of the Russian Federation 2020-07-24]. 2020. — 48 p. — URL: http://www.kremlin.ru/acts/bank/45796. (accessed: 05.07.25). [in Russian]

3. Russian Federation. Federal'ny'j zakon ot 02.07.2021 No 331-FZ «O vnesenii izmenenij v otdel'ny'e zakonodatel'ny'e akty' Rossijskoj Federacii v svyazi s prinyatiem Federal'nogo zakona «Ob e'ksperimental'ny'x pravovy'x rezhimax v sfere cifrovy'x innovacij v Rossijskoj Federacii» [Federal Law of 02.07.2021 No. 331-FZ "On Amendments to Certain Legislative Acts of the Russian Federation in Connection with the Adoption of the Federal Law" On Experimental Legal Regimes in the Field of Digital Innovations in the Russian Federation "] : Federal Law №331-ФЗ : [accepted by State Duma of the Federal Assembly of the Russian Federation 2021-06-16 : approved by Federation Council of the Federal Assembly of the Russian Federation 2021-06-23]. 2021. — 44 p. — URL: http://publication.pravo.gov.ru/Document/View/0001202107020046. (accessed: 05.07.25). [in Russian]

4. GOST R 59277-2020. Sistemy' iskusstvennogo intellekta. Klassifikaciya sistem iskusstvennogo intellekta [GOST R 59277-2020. Artificial intelligence systems. Classification of artificial intelligence systems]. — Introduced 2020-12-23. — Moscow: Standartinform, 2021. — 16 P. [in Russian]

5. GOST R 59898-2021. Ocenka kachestva sistem iskusstvennogo intellekta. Obshhie polozheniya [GOST R 59898-2021. Assessing the quality of artificial intelligence systems. General provisions]. — Introduced 2021-11-26. — Moscow: Rossijskij institut standartizacii, 2021. — 24 P. [in Russian]

6. GOST R 59276-2020. Sistemy' iskusstvennogo intellekta. Sposoby' obespecheniya doveriya. Obshhie polozheniya [GOST R 59276-2020. Artificial intelligence systems. Ways to ensure trust. General provisions]. — Introduced 2020-12-23. — Moscow: Standartinform, 2021. — 16 P. [in Russian]

7. GOST R 59926-2021 Informacionny'e texnologii. E'talonnaya arxitektura bol'shix danny'x. Chast' 2. Varianty' ispol'zovaniya i proizvodny'e trebovaniya [GOST R 59926-2021 Information Technologies. Big data reference architecture. Part 2. Use Cases and Derivative Requirements]. — Introduced 2022-03-01. — Moscow: Standartinform, 2022. — 294 P. [in Russian]

8. GOST R 70466-2022/ISO/IEC TR 205471:2020 Informacionny'e texnologii. E'talonnaya arxitektura bol'shix danny'x. Chast' 1. Struktura i process primeneniya (ISO/IEC TR 20547-1:2020) [GOST R 70466-2022/ISO/IEC TR 205471:2020 Information Technologies. Big data reference architecture. Part 1. Structure and application process (ISO/IEC TR 20547-1: 2020)]. — Introduced 2022-11-08. — Moscow: Rossijskij institut standartizacii, 2022. — 20 P. [in Russian]

9. Russian Federation. Perspektivnaya programma standartizacii po prioritetnomu napravleniyu «Iskusstvenny'j intellekt» na period 2021–2024 gody' [Promising standardization program in the priority area "Artificial Intelligence" for the period 2021-2024] : Resolution of the Government of Russia 2020. — URL: https://www.economy.gov.ru/material/file/28a4b183b4aee34051e85ddb3da87625/20201222.pdf. (accessed: 05.07.25). [in Russian]

10. PNST 776-2022 Informacionny'e texnologii. Intellekt iskusstvenny'j. Upravlenie riskami [PNST 776-2022 Information Technology. Artificial intelligence. Risk management]. — Introduced 2022-11-02. — Moscow: Rossijskij institut standartizacii, 2022. — 28 P. [in Russian]

11. Samojlov A.V. Texnologii iskusstvennogo intellekta: vozmozhnosti ili ugrozy' [Artificial intelligence technologies: opportunities or threats] / A.V. Samojlov // HI-HUME JOURNAL. — 2023. — 3. — P. 67–71. — URL: https://hi-hume.ru/files/files/HHJ_2023_03(3).pdf (accessed: 26.02.26). [in Russian]

12. Gibadullin R.F. Analiz parametrov promy'shlenny'x setej s primeneniem nejrosetevoj obrabotki [Neural Network Data Processing for Analysis of the Industrial Networks Parameters] / R.F. Gibadullin, D.V. Lekomcev, M.Yu. Peruxin // Artificial intelligence and decision-making. — 2020. — 1. — P. 80–87. — URL: http://www.isa.ru/aidt/2020-01/80_87.pdf (accessed: 11.08.25). — DOI: 10.14357/20718594200108 [in Russian]

13. Manyika J. Big Data: The Next Frontier for Innovation, Comptetition, and Productivity / J. Manyika, B. Brown, J. Bughin et al. // Discover scientific knowledge and stay connected to the world of science; — 2011: Discover scientific knowledge and stay connected to the world of science, 2011. — URL: https://www.researchgate.net/publication/260480165_Big_Data_The_Next_Frontier_for_Innovation_Comptetition_and_Productivity. (accessed: 31.03.26).

14. Russell S.J. Artificial Intelligence: A Modern Approach (4th ed.). Pearson. / S.J. Russell, P. Norvig. — 2021: SPi Global, 2021. — 117 p. — URL: https://clck.ru/3UD6ke. (accessed: 25.03.26).

15. GOODFELLOW I Deep Learning (Adaptive Computation and Machine Learning series) [Deep Learning (Adaptive Computation and Machine Learning series)] / I Goodfellow, Y Bengio, A Courville. — 2016: AMAZON, 2016. — 781 p. — URL: https://www.deeplearningbook.org/. (accessed: 31.03.26). [in Russian]

16. Floridi L. The Ethics of Artificial Intelligence / L. Floridi. — Oxford: University press, 2019. — 28 p. — URL: https://clck.ru/3UD6av. (accessed: 26.02.26).

17. Szegedy C Intriguing properties of neural networks / C Szegedy, W Zaremba, I Sutskever et al. // Cornelll University; — 2014: Cornell University, 2014. — URL: https://arxiv.org/abs/1312.6199. (accessed: 31.03.26).

18. Ponkin I.V. Mashinochitaemoe pravo, cifrovy'e modeli-dvojniki, cifrovaya formalizaciya i cifrovaya onto-inzheneriya v prave [Machine-readable law, digital twin models, digital formalization and digital onto-engineering in law] / I.V. Ponkin, A.I. Lapteva. — Moscow: Konsorcium «Analitika. Pravo. Cifra», 2021. — 174 p. — URL: https://clck.ru/3UD6fX. (accessed: 26.02.26). [in Russian]

19. Neznamov A Reakciya otrasli: chto ozhidaetsya ot novogo rossijskogo regulirovaniya II [Industry reaction: what to expect from the new Russian AI regulations] / A Neznamov. // ICT.Moscow; — Moscow: ICT.MOSCOW, 2025. [in Russian]