Профессиональное образование в современном мире
ISSN 2224-1841 (print)
2026. Т. 16, №1. С. 12–19
https://doi.org/10.20913/2224-1841-2026-1-2

Professional education in the modern world
ISSN 2224-1841 (print)
2026, vol. 16, no. 1, pp. 12–19
https://doi.org/10.20913/2224-1841-2026-1-2

I ФИЛОСОФИЯ PHILOSOPHY

DOI: 10.20913/2224-1841-2026-1-2
УДК 004.8

Оригинальная статья

От цифрового разрыва к цифровому суверенитету: обеспечение суверенитета образовательных данных в условиях использования зарубежных ИИ-сервисов

Е. Ф. Мороз
Красноярский институт железнодорожного транспорта
Красноярск, Российская Федерация
e-mail: moroslena@yandex.ru
ORCID: 0000-0002-7504-7140

Аннотация. *Введение.* Понятие «цифровой суверенитет образовательных данных» подразумевает сохранение контроля над критически важными данными в условиях глобальной цифровизации. Использование зарубежных ИИ-сервисов в образовании создает парадокс: устраняя традиционный «цифровой разрыв», оно порождает новую угрозу – утрату суверенитета над персональными данными и интеллектуальной собственностью. *Постановка задачи.* Цель исследования – разработка многоуровневой стратегии обеспечения суверенитета образовательных данных для российской системы образования. Для этого необходимо проанализировать эволюцию цифрового разрыва, систематизировать риски использования зарубежных ИИ-сервисов и разработать комплексную модель противодействия. *Методика и методология исследования.* Методологическую основу составили системный подход, сравнительно-правовой анализ и моделирование рисков. Системный подход позволил рассмотреть проблему как комплекс взаимосвязанных элементов, а правовой анализ выявил пробелы в законодательстве о защите образовательных данных. *Результаты.* Основным результатом является разработанная многоуровневая стратегия, включающая государственно-правовой, институциональный и технологический уровни. На государственном уровне предложены меры нормативно-правового регулирования, на институциональном – модели корпоративных политик для вузов, на технологическом – внедрение отечественных защищенных ИИ-платформ. *Выводы*. Результаты имеют практическую ценность для формирования национальной политики в области цифрового образования.

Ключевые слова: социальная философия, цифровой суверенитет, образовательные данные, искусственный интеллект, цифровой разрыв, информационная безопасность, персональные данные, технологическая независимость

Для цитирования: *Мороз Е. Ф.* От цифрового разрыва к цифровому суверенитету: обеспечение суверенитета образовательных данных в условиях использования зарубежных ИИ-сервисов // Профессиональное образование в современном мире. 2026. Т. 16, №1. С. 12–19. DOI: https://doi.org/10.20913/2224-1841-2026-1-2

DOI: 10.20913/2224-1841-2026-1-2

Full Article

From digital divide to digital sovereignty: Safeguarding educational data sovereignty in the context of using foreign AI services

Moros, E. F.
Krasnoyarsk Rail Transport Institute
Krasnoyarsk, Russian Federation
e-mail: moroslena@yandex.ru
ORCID: 0000-0002-7504-7140

Abstract. *Introduction.* The concept of «digital sovereignty of educational data» implies maintaining control over critically important data in the context of global digitalization. The use of foreign AI services in education creates a paradox: while eliminating the traditional «digital divide», it gives rise to a new threat – the loss of sovereignty over personal data and intellectual property. *Purpose setting.* The aim of the research is to develop a multi-level strategy for ensuring the sovereignty of educational data for the Russian education system. This requires analyzing the evolution of the digital divide, systematizing the risks of using foreign AI services, and developing a comprehensive counteraction model. *Methodology and methods of the study.* The methodological basis consisted of a systems approach, comparative legal analysis, and risk modeling. The systems approach allowed for considering the problem as a set of interconnected elements, while the legal analysis revealed gaps in the legislation on the protection of educational data. *Results.* The main result is the developed multi-level strategy, which includes state-legal, institutional, and technological levels. At the state level, measures for regulatory and legal framework are proposed; at the institutional level, models of corporate policies for universities are suggested; and at the technological level, the implementation of domestic secure AI platforms is recommended. *Conclusion.* The results have practical value for shaping national policy in the field of digital education.

Keywords: social philosophy, digital sovereignty, educational data, artificial intelligence, digital divide, information security, personal data, technological independence

Citation: Moros, E. F. [From digital divide to digital sovereignty: Safeguarding educational data sovereignty in the context of using foreign AI services]. *Professional education in the modern world,* 2026, vol. 16, no. 1, pp. 12–19. DOI: https://doi.org/10.20913/2224-7515-1841-1-2

Введение. В образовательный процесс активно внедряются зарубежные сервисы на основе искусственного интеллекта (ИИ), такие как ChatGPT, Midjourney, Gemini и многие другие. Это создает парадоксальную ситуацию.

С одной стороны, они открывают доступ к передовым технологиям, нивелируя классический «цифровой разрыв» (digital divide), понимаемый как неравенство в доступе к цифровым технологиям. Как отмечает С. И. Черных, мы действительно наблюдаем устойчивую тенденцию к изменению обучения под влиянием приложений ИИ [1, с. 12], что формально сокращает этот разрыв. С другой стороны, порождается новая, более глубокая форма разрыва – утрата цифрового суверенитета (digital sovereignty) и, в частности, суверенитета данных (data sovereignty) [2].

Проблема заключается в том, что массовое и часто бесконтрольное использование глобальных ИИ-платформ приводит к трансграничной утечке образовательных данных (включая персональные данные, интеллектуальные продукты студентов и педагогов, метрики обучения), которые попадают под юрисдикцию других государств и используются для обучения коммерческих моделей без явного согласия субъектов данных [3, с. 87].

Несмотря на наличие работ, посвященных общим рискам цифровой зависимости [4] и безопасности данных [2; 5], комплексная стратегия обеспечения суверенитета именно образовательных данных при использовании зарубежного ИИ остается неразработанной. Существующие публикации не предлагают моделей для перехода от осознания рисков к их практическому парированию, что и определяет научную проблему данного исследования.

Постановка задачи. Основной целью исследования является разработка многоуровневой стратегии обеспечения цифрового суверенитета образовательных данных для российской системы образования в условиях активного использования зарубежных ИИ-сервисов. Достижение этой цели напрямую связано с решением ряда фундаментальных задач: 1. Проанализировать эволюцию концепции «цифрового разрыва» и его

трансформацию в проблему «цифрового суверенитета» применительно к сфере образования. 2. Систематизировать и классифицировать ключевые риски, связанные с утратой суверенитета образовательных данных при использовании глобальных ИИ-платформ (трансграничная утечка данных, утрата интеллектуальной собственности, правовая неопределенность). 3. Разработать комплексную многоуровневую модель (стратегию) противодействия угрозам цифрового суверенитета, включающую государственно-правовой, институциональный и технологический уровни. 4. Предложить конкретные практические меры для каждого уровня стратегии, включая рекомендации по нормативно-правовому регулированию, корпоративным политикам образовательных организаций и внедрению защищенных отечественных технологических решений.

Методика и методология исследования. Методологическую основу исследования составил комплекс взаимодополняющих подходов. Ведущим выступил системный подход, позволивший рассмотреть проблему обеспечения суверенитета образовательных данных как целостный объект, состоящий из взаимосвязанных элементов: правового поля, институциональных практик и технологической инфраструктуры.

В рамках исследования применен сравнительно-правовой анализ, направленный на выявление пробелов в российском и международном законодательстве о защите данных и использовании искусственного интеллекта. Для систематизации угроз использовался метод моделирования рисков, позволивший структурировать их по вероятности возникновения и масштабу последствий.

На различных этапах работы применялись общенаучные методы: анализ научной литературы, нормативных документов и политик зарубежных ИИ-сервисов, а также синтез полученных данных для разработки целостной стратегии.

Результаты. В работе Е. А. Басовой концепция «цифрового разрыва» определяется как фундаментальное неравенство в доступе к информационно-коммуникационным технологиям [6, с. 11] Однако, как показывают современные исследования, динамика технологического развития, и в особенности экспансия искусственного интеллекта, привела к качественной трансформации данного понятия [7, с. 58].

Первоначально, в конце XX – начале XXI в., цифровой разрыв понимался преимущественно в количественном и инфраструктурном ключе [8, с. 964]. Схожей позиции придерживаются и другие ученые, трактуя его как неравенство в доступе к цифровым технологиям и интернету между различными географическими регионами, социально-экономическими группами или поколениями [9]. В этот период основной задачей считалось преодоление разрыва путем расширения сетевой инфраструктуры и обеспечения доступности устройств [10]. Казалось, что массовое распространение глобальных цифровых платформ и сервисов, включая социальные сети и облачные решения, является универсальным ответом на эту проблему, нивелируя базовое технологическое неравенство.

Однако по мере всеобщей цифровизации фокус сместился с проблемы доступа на проблему качества и характера использования технологий. Эту тенденцию фиксирует исследование И. В. Деревцовой и др., где цифровое неравенство рассматривается как угроза экономической безопасности [11]. Сформировалась концепция второго уровня цифрового разрыва, который связан уже не с наличием инфраструктуры, а с разрывом в цифровых компетенциях, что находит отражение в методиках измерения цифровых разрывов в бизнес-секторе [12]. По мнению Е. Г. Киселевой, именно на этой стадии стали очевидны риски, связанные с зависимым характером цифровизации. Массовое принятие внешних, часто зарубежных, технологических решений, призванное сократить разрыв в компетенциях, породило новую, системную уязвимость [13, с. 74]. Это привело к становлению современной, третьей фазы эволюции понятия. В рамках данной фазы, как отмечается в исследованиях, цифровой разрыв трансформируется в проблему цифрового суверенитета и, в частности, суверенитета данных [14, с. 59].

Если первоначальный разрыв был проблемой «иметь или не иметь», а разрыв второго уровня – проблемой «уметь или не уметь», то современный вызов в свете исследований можно сформулировать как проблему «контролировать или быть контролируемым». Угрозы суверенитету данных становятся прямым следствием кажущегося преодоления предыдущих форм разрыва. Ярким примером этого парадокса служит активное использование глобальных ИИ-сервисов в таких чувствительных сферах, как образование [15].

Эволюция цифрового разрыва представляет собой движение от периферийных проблем доступа к центральной проблеме управления и контроля в цифровой среде. Современный разрыв проявляется как асимметрия между теми, кто обладает технологическим суверенитетом и контролирует ключевые данные и алгоритмы, и теми, кто, пользуясь внешними сервисами, делегирует этот контроль.

Эта новая реальность приводит к парадоксу: стремление получить мгновенный доступ к передовым технологиям (то есть преодолеть разрывы первого и второго уровня) оборачивается утратой контроля над критическими активами – образовательными данными. В результате массовое ис-

пользование зарубежных ИИ-сервисов в образовательной сфере порождает комплекс взаимосвязанных угроз суверенитету образовательных данных, которые выходят далеко за рамки простых рисков конфиденциальности.

В основе проблемы лежат юридико-правовые и юрисдикционные риски, обусловленные подчинением данных иностранному законодательству. Как отмечает Н. А. Шебанова, принятие в ЕС Общего регламента по защите данных (GDPR) создало правовое поле, имеющее приоритет над национальными законами, что является наглядным примером подобной коллизии. Тот факт, что инфраструктура и компании-операторы находятся под юрисдикцией других государств, создает прямую коллизию с национальными нормами о защите персональных данных [16, с. 71].

Критическую угрозу представляет экстерриториальное действие законов, подобных американскому CLOUD Act, который позволяет правоохранительным органам США получать доступ к данным, хранящимся на серверах где бы то ни было, если ими владеет американская компания. Как справедливо отмечает в своем исследовании С. В. Гландин, экстерриториальное применение американского законодательства создает значительные правовые риски для российских резидентов [17, с. 106]. Как отмечают исследователи, данный закон обязывает поставщиков услуг, подпадающих под юрисдикцию США, предоставлять данные по запросу властей независимо от того, находятся ли эти данные на территории США или за их пределами. Это не только ставит под сомнение возможность соблюдения российского законодательства, но и создает правовую неопределенность в отношении статуса данных. Аналитики подчеркивают, что CLOUD Act создает значительную юридическую неопределенность для глобально операционных компаний, которые сталкиваются с противоречивыми юридическими требованиями, а также ведет к прямым и фундаментальным конфликтам с установленными режимами защиты данных других стран.

Пользовательские соглашения зарубежных платформ де-факто переводят интеллектуальные продукты студентов и педагогов – уникальные решения, аналитические записи, методические материалы – в категорию корпоративной собственности, используемой для тренировки коммерческих моделей без явного и информированного согласия субъектов.

Непосредственно с этим связаны технологические и архитектурные риски, проистекающие из закрытости и централизованности глобальных ИИ-платформ. Трансграничная передача и хранение образовательных данных на зарубежных серверах объективно повышают уязвимость перед кибератаками, несанкционированным доступом и утечками. Актуальность данной угрозы подтверждается статистикой: против России действует более миллиона хакеров, а крупнейшие компании, такие как Сбербанк, ежесуточно отражают тысячи атак. Однако более глубокая угроза заключается в «эффекте черного ящика»: непрозрачность алгоритмов, принимающих решения в образовательном процессе (например, при оценке знаний или формировании индивидуальных траекторий), лишает педагогическое сообщество возможности проверить их обоснованность, объективность и отсутствие скрытых смещений. Образовательное учреждение, делегирующее столь важные функции неподконтрольной и неподотчетной системе, теряет технологический суверенитет над собственными процессами.

Долгосрочные последствия порождают экономико-стратегические риски, главный из которых – формирование устойчивой технологической зависимости. Интеграция учебных курсов, методик и управленческих решений вокруг конкретного зарубежного сервиса создает эффект «экосистемной ловушки» (vendor lock-in), когда затраты на переход на альтернативную, в том числе отечественную, платформу становятся prohibitively высокими.

Критики CLOUD Act отмечают, что этот закон вызвал опасения относительно доверия к американским поставщикам технологий и может наносить ущерб глобальной конкурентоспособности американских облачных и технологических поставщиков, поскольку клиенты могут выбирать поставщиков в странах, предлагающих более сильную защиту приватности [18]. Это не только подавляет развитие национальной ИИ-инфраструктуры, но и приводит к стратегическому истощению ресурса: данные, генерируемые российской системой образования, становятся топливом для улучшения иностранных коммерческих продуктов, укрепляя тем самым конкурентные позиции и технологическое лидерство других стран.

Наконец, наиболее латентными, но фундаментальными являются социокультурные и педагогические риски. Как показано в исследовании П. М. Лукичёва и О. П. Чекмарева, поскольку зарубежные ИИ-модели обучаются на массивах данных, репрезентирующих определенные культурные и ценностные контексты, их выводы могут неявно пропагандировать чуждые идеологические установки, искаженные трактовки исторических событий и социальных норм [19, с. 469]. Это создает угрозу «цифрового колониализма», при котором через, казалось бы, нейтральные образовательные технологии происходит эрозия культурной и ценностной идентичности. В педагогическом аспекте, по мнению И. В. Филимоно-

вой наблюдается деградация профессионального суверенитета педагога, чьи экспертные функции – от разработки методик до оценки результатов – вытесняются и диктуются алгоритмами, логика которых неподконтрольна и непонятна [20].

Для парирования выявленных рисков необходима комплексная стратегия, реализуемая на взаимосвязанных уровнях. Ключевой основой предлагаемой модели является обеспечение цифрового суверенитета, который, по обоснованному в научной литературе мнению, «заключается в соединении национальной инфраструктуры, нормативной правовой базы и профессиональных компетенций в цифровой сфере». Исходя из этого, предлагаемая модель предполагает синхронные действия на государственно-правовом, институциональном и технологическом уровнях, формируя тем самым устойчивый контур цифрового суверенитета [21, с. 40].

Фундаментом всей системы является государственно-правовой уровень, где ключевая роль отводится формированию четкого нормативного поля. Прежде всего это требует разработки и внедрения специализированных стандартов и регламентов, прямо регулирующих использование зарубежных ИИ-сервисов в образовательных организациях [22, с. 5]. Подобные регламенты должны устанавливать юридически обязывающие требования, такие как обязательная локализация серверов для обработки образовательных данных и получение явного информированного согласия всех субъектов образовательного процесса на сбор и использование их данных. Это является практическим воплощением цифрового суверенитета, который понимается как способность государства устанавливать обязательные для исполнения правила игры в цифровой среде, исходя из необходимости формирования собственного технологического разнообразия и компетенций.

Кроме того, необходима разработка и сертификация белых (рекомендованных) и черных (запрещенных) списков ИИ-сервисов, основанных на аудите их политик безопасности и соответствия национальному законодательству, что создает прозрачные и понятные ориентиры для образовательных учреждений.

На институциональном уровне стратегия фокусируется на выработке конкретных механизмов реализации государственных установок внутри образовательных организаций. Как отмечает руководитель группы правового обеспечения Сколтеха Дмитрий Голованов, университет создал «контур правового регулирования, безусловно, позитивно настроенный к ИИ, но все-таки определяющий набор правил. Ключевыми направлениями становятся разработка и принятие внутренних политик и регламентов использования ИИ, которые детализировали бы процедуры работы с данными, оценивали риски конкретных сервисов и закрепляли принципы академической добросовестности.

Не менее важной задачей является комплексная программа повышения цифровой грамотности педагогов и административного персонала, направленная на формирование критического понимания принципов работы ИИ, связанных с ними рисков и мер защиты данных. Ключевой задачей становится преодоление «цифрового разрыва» второго уровня, который, как подчеркивают Д. Е. Добринская и Т. С. Мартыненко, «связан с дифференциацией практик применения ИКТ и последствий их реализации» [23, с. 112]. Это означает, что на первый план выходит не столько умение пользоваться технологиями, сколько критическое понимание их работы и способность сохранять над ними содержательный контроль.

Технологический уровень стратегии обеспечивает практический инструментарий для реализации правовых и институциональных норм. Центральным элементом здесь является ускоренное развитие и внедрение отечественных ИИ-платформ и образовательных экосистем, развернутых на территории страны и подконтрольных национальным юрисдикциям. Как отмечается в аналитической записке, для стран, стремящихся к технологическому суверенитету, подобные меры являются системным решением для снижения внешней зависимости и защиты национальных интересов в цифровой сфере [24]. Это позволит не только обеспечить физический контроль над данными, но и гарантировать их соответствие культурным и педагогическим стандартам.

С технологической точки зрения приоритет должен быть отдан решениям, поддерживающим архитектурные принципы конфиденциальности, такие как федеративное машинное обучение (federated learning). Эта технология, как определяют ее М. А. Ефремов и И. И. Холод, позволяет осуществлять «коллективное машинное обучение на распределенных обучающих наборах данных без их передачи в единое хранилище» [25, с. 263]. Такой подход, по мнению Европейского надзорного органа по защите данных (EDPS), является перспективным для минимизации рисков для конфиденциальности, поскольку необработанные данные остаются локализованными, а между участниками передаются только обновления модели [26]. Это полностью решает задачу обучения моделей ИИ без вывода исходных данных за пределы образовательного учреждения.

Выводы. Таким образом, проведенное исследование позволяет утверждать, что обеспечение цифрового суверенитета образовательных данных требует перехода от констатации рисков к построению целостной системы защиты. Разработанная многоуровневая стратегия, синтезирующая

государственно-правовые, институциональные и технологические меры, создает методологический фундамент для формирования защищенной образовательной экосистемы. Ее практическая реализация позволит не только минимизировать зависимость от иностранных ИИ-сервисов, но и заложить основу для устойчивого развития национального образовательного пространства.

СПИСОК ЛИТЕРАТУРЫ

1. Черных С. И. Искусственный интеллект в изменении педагогического дизайна // Профессиональное образование в современном мире. 2024. Т. 14, №1. С. 10–16. DOI: https://doi.org/10.20913/2618-7515-2024-1-2
2. Семёнкина И. А., Павлова Т. А. Проблемы обеспечения цифрового суверенитета в сфере отечественного высшего образования // Мир педагогики и психологии: международный научно-практический журнал. 2022. № 04 (69). URL: https://scipress.ru/pedagogy/articles/problemy-obespecheniya-tsifrovogo-suvereniteta-v-sfere-otechestvennogo-vysshego-obrazovaniya.html?ysclid=mgi1r7urnx749283631 (дата обращения: 01.10.2025).
3. Чунгулова Г. К., Оразалиева Э. Н. Возможности и проблемы больших языковых моделей в образовании на примере ChatGPT // Наука и реальность. 2024. №4 (20). С. 85–91.
4. Ромашкина Г. Ф., Хузяхметов Р. Р. Риски интернет-зависимости: структура и особенности восприятия // Образование и наука. 2020. Т. 22, №8. С. 108–134. DOI: 10.17853/1994-5639-2020-8-108-134
5. Селюк А. С. Защита персональных данных в цифровом пространстве. Вестник Университета имени О. Е. Кутафина (МГЮА). 2023. № (2). С. 110–119. https://doi.org/10.17803/2311–5998.2023.102.2.110–119
6. Басова Е. А. Цифровое неравенство российских регионов: современные проблемы и пути преодоления // Вопросы территориального развития. 2021. Т. 9, №4. DOI: 10.15838/tdi.2021.4.59.4 URL: http://vtr.isert-ran.ru/article/29046 (дата обращения: 01.10.2025).
7. Земцов С. П., Демидова К. В., Кичаев Д. Ю. Распространение Интернета и межрегиональное цифровое неравенство в России: тенденции, факторы и влияние пандемии // Балтийский регион. 2022. Т. 14, №4. С. 57–78. DOI: 10.5922/2079-8555-2022-4-4
8. Дудин М. Н., Шкодинский С. В., Усманов Д. И. Оценка влияния цифрового неравенства на уровень социально-экономического развития регионов Российской Федерации // Вопросы инновационной экономики. 2021. Т. 11, №3. С. 962–984. DOI: 10.18334/vinec. 11.3.113452
9. Гулина С. Т., Мусина Д. Р. Цифровое неравенство как препятствие для развития регионов и отраслей // Human Progress. 2024. Т. 10. Вып. 5. С. 6. URL: fhttps://progress-human.com/images/2024/Tom10_5/Gulina.pdf (дата обращения: 01.10.2025).
10. Вартанова Е. Л. Медиаэкономика зарубежных стран. М.: Аспект Пресс, 2010. 335 с.
11. Деревцова И. В., Внукова Я. А., Головащенко Е. А. Проблема цифрового неравенства регионов России как угроза экономической безопасности // Baikal Research Journal. 2021. Т. 12. №2.
12. Якимова В. А., Хмура С. В. Измерение цифровых экономических разрывов в бизнес-секторе региональной экономики // Журнал Новой экономической ассоциации. 2023. №4 (61). С. 70–92.
13. Киселева Е. Г. Влияние цифровизации на инвестиционный потенциал города. Финансы: теория и практика. 2020. № 24 (5). С. 72–83. DOI: 10.26794/2587-5671-2020-24-5-72-83
14. Ребро О., Гладышева А., Сучков М., Сушенцов А. Категория «Цифрового суверенитета» в современной мировой политике вызовы и возможности для России. Международные процессы. 2021. № 19 (4). С. 47–67. DOI: https://doi.org/10.17994/IT.2021.19.4.67.6
15. Морозова С. С., Курочкин А. В. Цифровая колониализация как угроза национальной безопасности // Политическая экспертиза: Политекс. 2024. Т. 20, №1.
16. Шебанова Н. А. Охрана персональных данных: опыт международного регионального сотрудничества // Международное право и международные организации. 2020. №2. С. 69–87. DOI: 10.7256/2454–0633.2020.2.32597 URL: https://nbpublish.com/library_read_article.php?id=32597
17. Гландин С. В. Экстерриториальность американских санкций в действии // Международное правосудие. 2018. №2. С. 105–122.
18. Dinic M. The CLOUD Act & Data Archiving // Jatheon. 2024. 12 ноября. URL: https://jatheon.com/blog/cloud-act-data-archiving/ (дата обращения: 07.10.2025).
19. Лукичев П. М., Чекмарев О. П. Риски применения искусственного интеллекта в системе высшего образования // Вопросы инновационной экономики. 2024. Т. 14, №2. С. 463–482. DOI: 10.18334/vinec.14.2.120731
20. Филимонова И. В. Этическая сторона использования искусственного интеллекта в образовании // Вестник евразийской науки. 2024. Т. 16, № S1. URL: https://esj.today/PDF/64FAVN124.pdf
21. Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12: Политические науки. 2022. №2. С. 31–45.

22. Зажигалкин А. В., Мансуров Т. Т., Мерецков О. В. Регулирование искусственного интеллекта в образовании // Компетентность. 2024. №6. С. 3–10. DOI: 10.24412/1993-8780-2024-6-03-10
23. Добринская Д. Е., Мартыненко Т. С. Вестник РУДН. Серия: Социология. 2019. Т. 19, №1. С. 108–120.
24. Моисеева Д. Э. Цифровое управление в ЕС: между правилами и инновациями: аналитическая записка № 61/2025 // Российский совет по международным делам (РСМД). 2025. URL: https://drive.google.com/file/d/1qI0jqwNox2tWLco1SClwlp8fq18NlOSs/view (дата обращения: 08.10.2025).
25. Ефремов М. А., Холод И. И. Разработка архитектуры универсального фреймворка федеративного обучения // Программные продукты и системы. 2022. Т. 35, №2. С. 263–272. DOI: 10.15827/ 0236-235X.138.263–272
26. Generative AI and the EUDPR – First EDPS Orientations issued for ensuring data protection compliance // Rouse. 2024. URL: https://rouse.com/insights/news/2024/generative-ai-and-the-eudpr-first-edps-orientations-issued-for (дата обращения: 08.10.2025).

REFERENCES

1. Chernykh S. I. Artificial Intelligence in Changing Pedagogical Design. *Professional education in the modern world*, 2024, no. 14 (1), pp. 10–16. (in Russ.)
2. Semenkina I. A., Pavlova T. A. Problems of ensuring digital sovereignty in the field of domestic higher education. *World of pedagogy and psychology: international scientific-practical journal*, 2022, no. 04 (69). URL: https://scipress.ru/pedagogy/articles/problemy-obespecheniya-tsifrovogo-suvereniteta-v-sfere-otechestvennogo-vysshego-obrazovaniya.html?ysclid=mgi1r7urnx749283631 (accessed 10.01.2025). (in Russ.)
3. Chungulova G. K., Orazalieva E. N. Opportunities and challenges of large language models in education on the example of ChatGPT. *Science and reality*, 2024, no. 4 (20), pp. 85–91. (in Russ.)
4. Romashkina G. F., Khuzyakhmetov R. R. Risks of internet addiction: structure and perception features. *Education and science*, 2020, vol. 22, no. 8, pp. 108–134. DOI: 10.17853/1994-5639-2020-8-108-134. (in Russ.)
5. Selyuk A. S. Personal data protection in the digital space. *Kutafin University (MSAL) Bulletin*. 2023, no. (2), pp.110–119. URL: https://doi.org/10.17 803/2311–5998.2023.102.2.110–119 (in Russ.)
6. Basova E. A. Digital inequality of Russian regions: current problems and ways t o overcome them. *Territorial Development issues*, 2021, vol. 9, no. 4. DOI: 10.15838/tdi.2021.4.59.4. URL: http://vtr.isert-ran.ru/article/29 046. (in Russ.)
7. Zemtsov S. P., Demidova K. V., Kichaev D. Yu. The spread of the Internet and interregional digital inequality in Russia: trends, factors, and the impact of the pandemic. *Baltic Region*, 2022, vol. 14, no. 4, pp. 57–78. DOI: 10.5922/2079-8555-2022-4-4 (in Russ.)
8. Dudin M. N., Shkodinsky S. V., Usmanov D. I. Assessment of the impact ofdigital inequality on the level of socio-economic development of the regions of the Russian Federation. *Innovation economy issues,* 2021, vol. 11, no. 3, pp. 962–984. DOI: 10.18 334/vinec.11.3.113 452 (in Russ.)
9. Gulina S. T., Musina D. R. Digital inequality as an obstacle to the development of regions and industries. *Human progress*, 2024, vol. 10, issue 5, pp. 6. URL: fhttps://progress-human.com/images/2024/Tom10_5/Gulina.pdf (in Russ.)
10. Vartanova E. L. *Media Economics of Foreign Countries*. Moscow: Aspect Press Publ., 2010, 335 p. (in Russ.)
11. Derevtsova I. V., Vnukova Y. A., Golovashchenko E. A. The problem of digital inequality in Russian regions as a threat to economic security. *Baikal research journal*, 2021, vol. 12, no. 2. (in Russ.)
12. Yakimova V. A., Khmura S. V. Measuring digital economic gaps in the business sector of regional economy. *Journal of the new economic association*, 2023, no. 4 (61), pp. 70–92. (in Russ.)
13. Kiseleva E. G. The impact of digitalization on the investment potential of the city. *Finance: theory and practice*, 2020, no. 24 (5), pp. 72–83. DOI: 10.26794/2587-5671-2020-24-5-72-83 (in Russ.)
14. Rebro O., Gladysheva A., Suchkov M., Sushentsov A. The category of «digital sovereignty» in modern world politics: challenges and opportunities for Russia. *International trends*, 2021, no. 19 (4), pp. 47–67. URL: https://doi.org/10.17 994/IT.2021.19.4.67.6 (in Russ.)
15. Morozova S. S., Kurochkin A. V. Digital colonization as a threat to national security. *Political expertise: politex*, 2024, vol. 20, no. 1. (in Russ.)
16. Shebanova N. A. Personal data protection: experience of international regional cooperation. *International law and international organizations*, 2020, no. 2, pp. 69–87. DOI: 10.7256/2454–0633.2020.2.32 597 URL: https://nbpublish.com/library_read_article.php?id=32 597 (in Russ.)
17. Glandin S. V. Extraterritoriality of US sanctions in action. *International justice*, 2018, no. 2, pp. 105–122. (in Russ.)
18. Dinic M. The CLOUD Act & Data Archiving. Jatheon, 2024, november 12. URL: https://jatheon.com/blog/cloud-act-data-archiving/ (accessed 10.07.2025).
19. Lukichev P. M., Chekmarev O. P. Risks of artificial intelligence application in the higher education system. *Innovation economy issues*, 2024, vol. 14, no. 2, pp. 463–482. DOI: 10.18334/vinec.14.2.120731 (in Russ.)

20. Filimonova I. V. Ethical aspects of artificial intelligence use in education. *Eurasian scientific journal*, 2024, vol. 16, no. S1. URL: https://esj.today/PDF/64FAVN124.pdf (in Russ.)
21. Kochetkov A. P., Maslov K. V. Digital sovereignty as the basis of Russia's national security in the global digital society. *Moscow university bulletin. Series 12: Political science*, 2022, no. 2, pp. 31–45. (in Russ.)
22. Zazhigalkin A. V., Mansurov T. T., Meretskov O. V. Regulation of Artificial Intelligence in Education, Kompetentnost'. Competency (Russia), 2024, no. 6, pp. 3–10. DOI: 10.24412/1993-8780-2024-6-03-10
23. Dobrinskaya D. E., Martynenko T. S. *RUDN Journal of Sociology*, 2019, vol. 19, no. 1, pp. 108–120. (in Russ.)
24. Moiseeva D. E. Digital governance in the EU: between rules and innovations: analytical note No. 61/2025. *Russian international affairs council (RIAC)*. 2025. URL: https://drive.google.com/file/d/1qI0jqwNox2tWLco1SClwlp-8fq18NlOSs/view (accessed: 10.08.2025). (in Russ.)
25. Efremov M. A., Kholod I. I. Development of the architecture of a universal federated learning framework. *Software & systems*, 2022, vol. 35, no. 2, pp. 263–272. DOI: 10.15827/0236-235X.138.263–272. (in Russ.)
26. Generative AI and the EUDPR – First EDPS Orientations issued for ensuring data protection compliance. *Rouse*. 2024. URL: https://rouse.com/insights/news/2024/generative-ai-and-the-eudpr-first-edps-orientations-issued-for (accessed 10.08.2025).

Информация об авторе

Мороз Елена Фёдоровна – кандидат философских наук, доцент, доцент кафедры управления персоналом, Красноярский институт железнодорожного транспорта (Российская Федерация, 660 029, г. Красноярск, ул. Новая заря, 2и, e-mail: moroslena@yandex.ru). ORCID: 0000-0002-7504-7140

Статья поступила в редакцию 13.10.2025
После доработки 19.03.2026
Принята к публикации 20.03.2026

Information about the author

Elena F. Moros – candidate of philosophical sciences, associate professor, associate professor at the department of personnel management, Krasnoyarsk Rail Transport Institute – Branch of Irkutsk State Transport University (2i Novaya Zarya Str., Krasnoyarsk, 660 029, Russian Federation, e-mail: moroslena@yandex.ru). ORCID: https://orcid.org/0000-0002-7504-7140

The paper was submitted 13.10.2025
Received after reworking 19.03.2026
Accepted for publication 20.03.2026