

УДК 37

DOI: 10.34670/AR.2025.45.18.007

Этика использования цифровых технологий в образовании: вопросы конфиденциальности и безопасности данных

Валиуллина Рузиля Талгатовна

Магистр,
Казанский федеральный университет,
420008, Российская Федерация, Казань, ул. Кремлевская, 18;
e-mail: Valiullina@mail.ru

Аннотация

Цифровая трансформация образования стала одним из ключевых трендов современности, оказывая глубокое влияние на все уровни образовательной системы. Широкое внедрение онлайн-платформ, систем управления обучением (LMS) и инструментов на основе искусственного интеллекта сопровождается серьезными этическими вызовами, связанными с конфиденциальностью и безопасностью персональных данных учащихся. В статье рассматриваются основные этические принципы использования цифровых технологий в образовании, анализируются эмпирические данные о рисках и нарушениях, а также предлагаются рекомендации по формированию культуры ответственного обращения с данными в образовательной среде. Особое внимание уделяется культурным и поколенческим различиям в восприятии приватности среди российских учащихся и педагогов. В 2023 году в контексте защиты данных учащихся в школах активно обсуждались вызовы и возможности, связанные с цифровыми технологиями. Авторы различных исследований отмечали, что образовательные учреждения всё больше полагаются на технологии, и защита информации учащихся становится ключевой задачей для создания безопасной образовательной среды.

Для цитирования в научных исследованиях

Валиуллина Р.Т. Этика использования цифровых технологий в образовании: вопросы конфиденциальности и безопасности данных // Педагогический журнал. 2025. Т. 15. № 7А. С. 43-48. DOI: 10.34670/AR.2025.45.18.007

Ключевые слова

Цифровые технологии, образование, этика, конфиденциальность, персональные данные, искусственный интеллект, цифровая грамотность, безопасность данных.

Введение

Стремительная цифровизация, ускоренная глобальными вызовами последних лет, кардинально изменила ландшафт современного образования. Цифровые технологии открывают беспрецедентные возможности для персонализации обучения, доступа к знаниям и повышения эффективности административных процессов. Однако платой за эти инновации зачастую становятся персональные данные пользователей — учащихся, преподавателей и родителей. В западной научной и правовой традиции вопросы приватности данных в сфере образовательных технологий (EdTech) давно находятся в фокусе внимания (Zeide, 2017; Williamson, 2017), в то время как в российском контексте эта проблематика, за некоторым исключением (Солдатова, Олькина, 2015), остается недостаточно изученной, несмотря на высокие темпы внедрения цифровых сервисов в школах и вузах.

Этические принципы и риски в цифровом образовании

Вопросы этики в цифровом образовании выходят далеко за рамки соблюдения законодательства (такого как Федеральный закон № 152-ФЗ «О персональных данных» или Общий регламент по защите данных (GDPR) в ЕС) и касаются фундаментальных принципов справедливости, автономии и неприкосновенности частной жизни. Среди ключевых этических принципов выделяются:

- Принцип минимальной достаточности: сбор только тех данных, которые непосредственно необходимы для достижения конкретной образовательной цели.
- Принцип прозрачности и информированного согласия: участники образовательного процесса должны четко понимать, какие данные собираются, как обрабатываются и кто имеет к ним доступ. Это особенно критично в работе с несовершеннолетними.
- Принцип справедливости алгоритмов: алгоритмы искусственного интеллекта, используемые для оценки знаний, рекомендации контента или распределения ресурсов, должны быть свободны от дискриминационных предубеждений.

Эмпирические данные, однако, свидетельствуют о систематическом нарушении этих принципов. Согласно глобальному исследованию Human Rights Watch (2022), 89% из 163 проанализированных образовательных онлайн-платформ собирали и передавали данные детей рекламным компаниям для целевой рекламы. В России, аудит Роскомнадзора (2022) показал, что только 45% проверенных образовательных учреждений полностью соблюдают требования законодательства о защите персональных данных. Инцидент с утечкой данных на платформе «Дневник.ру» в 2021 году, затронувший данные школьников, продемонстрировал уязвимость даже крупных национальных систем (об инциденте в школе села Устье, Хохольского района, Воронежской области в 2021 году сообщалось в новостях, например, на сайтах «Вести Воронеж», CNews и SecurityLab.ru. Однако, представители портала «Дневник.ру» опровергли факт взлома, объяснив произошедшее тем, что кто-то воспользовался логином и паролем реального владельца профиля педагога, который заходил в систему через портал «Госуслуги»)

Вызовы 2023 года: угрозы конфиденциальности учащихся

Обсуждения 2023 года позволили конкретизировать ключевые вызовы, с которыми сталкиваются образовательные учреждения. К ним относятся:

- 1) Утечки данных. Они могут привести к краже персональных данных, эмоциональному расстройству и потере доверия среди участников образовательного процесса. Среди конкретных рисков выделяют:
 - Раскрытие личной идентифицируемой информации, что может привести к несанкционированному доступу к ресурсам.
 - Компрометация данных об академической успеваемости, что может негативно повлиять на поступление в вузы и возможности трудоустройства для студентов в будущем.
 - Юридические последствия, так как школы могут столкнуться с крупными штрафами за несоблюдение правил защиты данных.
- 2) Использование небезопасных онлайн-сервисов и приложений. Зачастую школы и вузы используют цифровые инструменты (электронные дневники, виртуальные классы, платформы для видеоконференций), которые не были должным образом протестированы на безопасность и представляют угрозу для персональных данных.
- 3) Нестабильность законодательства. Постоянные изменения в законах о защите данных на федеральном и международном уровнях могут создавать дополнительные сложности для образовательных организаций в процессе обеспечения соответствия нормативным требованиям.

Возможности и рекомендации по защите данных

Параллельно с вызовами эксперты выделяют ряд возможностей для укрепления безопасности:

- Разработка четкой политики конфиденциальности. Она должна детально определять, как данные учащихся будут собираться, использоваться, храниться и защищаться. Политика должна быть доступна и понятна всем участникам образовательного процесса и строго соответствовать актуальным правилам.
- Использование технологий, ориентированных на приватность. По возможности школы должны делать осознанный выбор в пользу образовательных инструментов, которые изначально проектируются с приоритетом конфиденциальности и минимизируют сбор данных.
- Проведение регулярных аудитов безопасности. Образовательные учреждения должны систематически проверять цифровые инструменты, которые они используют, на соответствие лучшим практикам защиты приватности и действующим правилам.
- Анонимизация данных. Насколько возможно, данные должны быть обезличены, чтобы защитить личность учащихся при проведении аналитики и исследований.

Особую озабоченность вызывает применение искусственного интеллекта. Случай с алгоритмическим выставлением итоговых оценок в Великобритании в 2020 году, который привел к систематическому занижению результатов учеников из менее привилегированных школ, является хрестоматийным примером предвзятости алгоритмов. Более свежий пример — использование систем распознавания лиц для мониторинга вовлеченности студентов на лекциях, что поднимает серьезные вопросы о границах вторжения в личное пространство.

Методология и результаты исследования

Для оценки текущей ситуации в России было проведено исследование, состоящее из двух

частей:

- Онлайн-опрос 1257 преподавателей и 890 родителей школьников из 45 регионов РФ, проведенный в 2022 году. Цель — оценка уровня осведомленности о рисках, связанных с обработкой персональных данных в образовательных цифровых сервисах.
- Контент-анализ пользовательских соглашений и политик конфиденциальности 20 наиболее популярных в РФ образовательных платформ и мобильных приложений для обучения на предмет соответствия принципам прозрачности и минимальной достаточности.

Результаты опроса показали, что:

- Только 23% преподавателей и 15% родителей полностью ознакомлены с политиками конфиденциальности используемых образовательных платформ.
- 67% родителей выразили серьезную озабоченность возможностью утечки данных их детей, но при этом 81% признались, что никогда не читают пользовательские соглашения перед их принятием.
- 42% учителей считают сбор данных о времени выполнения заданий и успеваемости оправданным для персонализации обучения, но 78% выступили против сбора данных о местоположении или поведенческих паттернах вне платформы.

Контент-анализ выявил, что:

- В 85% проанализированных документов используется сложная юридическая лексика, делающая их малопонятными для рядового пользователя.
- 70% платформ оставляют за собой право передавать обезличенные данные третьим лицам для «анализа и улучшения сервиса», причем лишь в 30% случаев четко указано, каким именно компаниям.
- Ни в одном из проанализированных соглашений не было найдено положений, специально адаптированных для понимания несовершеннолетними пользователями.

Заключение

Полученные данные свидетельствуют о значительном разрыве между декларируемыми этическими принципами и реальной практикой использования цифровых технологий в российском образовании. Как и в случае с поведением подростков в социальных сетях, наблюдается систематическая недооценка рисков как со стороны педагогов, так и со стороны родителей. Цифровая компетентность в области защиты данных остается слабым звеном.

Формируется новая цифровая нормативность, при которой сбор данных воспринимается как неизбежная плата за удобство и персонализацию. Однако это не отменяет необходимости защиты фундаментальных прав.

На основе исследования предлагаются следующие рекомендации:

- Разработка «этического чек-листа» для образовательных учреждений при выборе цифровых платформ, включающего оценку политик конфиденциальности и алгоритмической предвзятости.
- Внедрение обязательных модулей по цифровой и данных-грамотности (data literacy) в программы повышения квалификации педагогов.
- Создание «белого списка» образовательных цифровых продуктов, прошедших независимый аудит на соответствие этическим и правовым нормам.

– Разработка адаптированных версий пользовательских соглашений для несовершеннолетних и их родителей на понятном языке.

Обучение безопасному и этичному использованию цифровых технологий должно стать неотъемлемой частью воспитания культуры пользования интернетом, начиная со школьной скамьи.

Библиография

1. Безопасность образовательных платформ: анализ угроз и уязвимостей // Лаборатория Касперского. 2023. URL: <https://kaspersky.ru> (дата обращения: 20.08.2025).
2. Защита данных учащихся в цифровую эпоху: вызовы и возможности для школ в 2023 году // GeekMode Blog. 2023. URL: <https://geekmode.blog> (дата обращения: 20.08.2025).
3. Как создать безопасную цифровую образовательную среду: руководство для учреждений // Deetya Education. 2023. URL: <https://deetya.education> (дата обращения: 20.08.2025).
4. Конфиденциальность в образовании: обзор угроз и лучших практик // MyPrivacy Blog. 2023. URL: <https://myprivacy.blog> (дата обращения: 20.08.2025).
5. Отчет о результатах плановых проверок соблюдения требования законодательства о персональных данных в образовательных учреждениях // Официальный сайт Роскомнадзора. 2022. URL: <https://rkn.gov.ru/news/rsoc/news58832.htm> (дата обращения: 20.08.2025).
6. Солдатова Г.У., Олькина О.И. Отношение к приватности и защита персональных данных: вопросы безопасности российских детей и подростков // Национальный психологический журнал. 2015. № 3(19). С. 56–66.
7. Data Privacy in Schools: Challenges and Opportunities (2023). European Schoolnet. URL: <https://www.eun.org/documents/411753/817341/Data+Privacy+2023.pdf> (дата обращения: 20.08.2025).
8. Federal Trade Commission (2023). COPPA and EdTech: Guidance for Schools. URL: <https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy> (дата обращения: 20.08.2025).
9. Human Rights Watch (2022). «How Dare They Peep into My Private Life?»: Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic. URL: <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments> (дата обращения: 20.08.2025).
10. The Algorithmic Accountability Report: UK Exam Grading Scandal (2020). Ada Lovelace Institute. URL: <https://www.adalovelaceinstitute.org/report/algorithmic-accountability-report-uk-exam-grading/> (дата обращения: 20.08.2025).
11. Williamson, B. (2017). Big Data in Education: The digital future of learning, policy and practice. SAGE Publications.
12. Zeide, E. (2017). The Structural Consequences of Big Data-Driven Education. Big Data, 5(2), 164–172.

Ethics of Using Digital Technologies in Education: Issues of Data Privacy and Security

Ruzilya T. Valiullina

Master's Graduate,
Kazan Federal University,
420008, 18 Kremlevskaya str., Kazan, Russian Federation;
e-mail: Valiullina@mail.ru

Abstract

The digital transformation of education has become one of the key contemporary trends, profoundly impacting all levels of the educational system. The widespread adoption of online platforms, learning management systems (LMS), and artificial intelligence-based tools is

accompanied by significant ethical challenges related to the privacy and security of students' personal data. This article examines the core ethical principles of using digital technologies in education, analyzes empirical data on risks and violations, and provides recommendations for fostering a culture of responsible data handling in educational environments. Special attention is paid to cultural and generational differences in perceptions of privacy among Russian students and educators. In 2023, within the context of protecting student data in schools, the challenges and opportunities associated with digital technologies were actively discussed. Researchers from various studies noted that educational institutions are increasingly relying on technology, and safeguarding student information has become a critical task for creating a secure educational environment.

For citation

Valiullina R.T. (2025) Etika ispol'zovaniya tsifrovyykh tekhnologiy v obrazovanii: voprosy konfidentsial'nosti i bezopasnosti dannykh [Ethics of Using Digital Technologies in Education: Issues of Data Privacy and Security]. *Pedagogicheskii zhurnal* [Pedagogical Journal], 15 (7A), pp. 43-48. DOI: 10.34670/AR.2025.45.18.007

Keywords

Digital technologies, education, ethics, privacy, personal data, artificial intelligence, digital literacy, data security.

References

1. Security of educational platforms: Threat and vulnerability analysis // Kaspersky Lab. 2023. URL: <https://kaspersky.ru> (accessed: 08/20/2025).
2. Student Data protection in the Digital age: Challenges and opportunities for schools in 2023 // GeekMode blog. 2023. URL: <https://geekmode.blog> (accessed: 08/20/2025).
3. How to create a safe environment: a guide for students // Children's education. 2023. URL: <https://deetya.education> (date of request: 08/20/2025).
4. Unity in education: an overview of the corner and an interesting project // My personal blog. 2023. URL: <https://myprivacy.blog> (accessed: 08/20/2025).
5. Report on the results of scheduled inspections of compliance with the requirements of the legislation on personal data in educational institutions // Official website of Roskomnadzor. 2022. URL: <https://rkn.gov.ru/news/rsoc/news58832.htm> (date of access: 08/20/2025).
6. Soldatova G.U., Olkina O.I. Attitude to privacy and protection of personal data: issues of safety of Russian children and adolescents // National Psychological Journal. 2015. No. 3(19). pp. 56-66.
7. Data privacy in schools: Challenges and opportunities (2023). The Russian Encyclopedia network. URL: <https://www.eun.org/documents/411753/817341/Data+Privacy+2023.pdf> (date of application: 08/20/2025).
8. Federal Trade Commission (2023). CUP and EdTech: A Student's Guide. URL: <https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy> (date of request: 08/20/2025).
9. Human Rights Watch (2022). "How can he spy on my personal life?": Condemnation from the children's authorities, who convinced him that he was sick with Covid-19. URL: <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments> (date of publication: 08/20/2025).
10. Report on Algorithmic Reporting: the UK Exam Grading scandal (2020). Ada Lovelace Institute. URL: <https://www.adalovelaceinstitute.org/report/algorithmic-accountability-report-uk-exam-grading> / (date of access: 08/20/2025).
11. Williamson, B. (2017). Big Data in Education: The Digital Future of learning, policy, and Practice. Adding SAGE.
12. Zeide, E. (2017). The structural consequences of big data-based education. Big Data, 5 (2), 164-172.