

Дата поступления рукописи в редакцию: 22.06.2026 г.
Дата принятия рукописи в печать: 14.07.2026 г.

DOI: 10.24412/2076-1503-2026-8-594-596

БЕЗЗАТЕЕВА Вероника Сергеевна,
старший преподаватель кафедры гражданского
права и кафедры информационной безопасности
Санкт-Петербургский государственный университет
аэрокосмического приборостроения,
e-mail: bezzateeva@inbox.ru

ДОКАЗАТЕЛЬСТВЕННАЯ СИЛА ЦИФРОВОГО СЛЕДА ОБУЧАЮЩЕГОСЯ В ОБРАЗОВАТЕЛЬНОМ СПОРЕ

Аннотация. В статье рассматривается цифровой след обучающегося как новый объект доказывания в спорах, возникающих из образовательных отношений. Показано, что журналы событий электронной информационно-образовательной среды, данные прокторинга, результаты онлайн-тестирования и алгоритмические отчеты одновременно являются цифровыми доказательствами, персональными данными и элементами образовательной документации. Предлагается модель паспорта образовательного цифрового следа, фиксирующая источник данных, способ идентификации, метаданные, условия хранения и порядок проверки автоматизированных выводов.

Ключевые слова: цифровой след; образовательный спор; электронное обучение; цифровые доказательства; персональные данные; прокторинг; искусственный интеллект.

BEZZATEEVA Veronika Sergeevna,
Senior Lecturer of the Department of Civil Law, Saint-Petersburg
State University of Aeronautical Instrumentation

THE EVIDENTIAL POWER OF A STUDENT'S DIGITAL FOOTPRINT IN AN EDUCATIONAL DISPUTE

Annotation. The article examines a learner's digital footprint as a new object of proof in disputes arising from educational relations. Logs of an electronic educational environment, proctoring data, online testing results and algorithmic reports are treated as digital evidence, personal data and educational records. The author proposes an educational digital footprint passport recording the data source, identification method, metadata, storage conditions and verification of automated conclusions.

Key words: digital evidence; electronic evidence; procedural reliability; electronic signature; screenshot; metadata; artificial intelligence.

Цифровизация образования изменила доказательственную основу споров между образовательной организацией и обучающимся. В электронной информационно-образовательной среде фиксируются входы в личный кабинет, время выполнения задания, попытки прохождения теста, загрузка файла, сообщения преподавателю, данные прокторинга и иные сведения. При конфликте о допуске к аттестации, академической задолженности, дисциплинарном взыскании, отчислении, либо о качестве образовательной услуги эти сведения начинают выполнять доказательственную функцию.

Статья 16 Федерального закона «Об образовании в Российской Федерации» допускает элек-

тронное обучение и дистанционные образовательные технологии. Постановление Правительства Российской Федерации от 11 октября 2023 г. № 1678 закрепило правила их применения и усилило значение информационных систем, цифровых сервисов, идентификации и аутентификации обучающихся, однако правовая оценка данных, возникающих внутри таких систем, остается менее определенной, чем порядок самой организации обучения.

Научная проблема состоит в том, что цифровой след обучающегося находится на пересечении нескольких режимов: для образовательной организации это учебная и управленческая информация, для обучающегося - персональные данные и

средство защиты права на образование, для суда - возможное цифровое доказательство.

Методология исследования

Исследование основано на формально-юридическом, системном и риск-ориентированном методах. Формально-юридический метод использован для анализа норм образовательного, гражданского, информационного и процессуального законодательства. Системный метод позволил рассмотреть цифровой след как объект, связанный с доказыванием, защитой персональных данных, локальным регулированием и качеством образовательной услуги. Риск-ориентированный метод применен для разграничения обычных данных электронной среды и сведений, полученных путем сложной автоматизированной обработки, включая прокторинг и инструменты искусственного интеллекта.

Основными целями исследования являются:

Целью настоящего исследования является разработка модели правовой верификации цифрового следа обучающегося в образовательном споре.

Цифровой след обучающегося целесообразно определять как совокупность сведений, создаваемых, передаваемых, сохраняемых или автоматически формируемых при участии обучающегося в образовательной информационной среде. В отличие от обычного электронного документа такой след часто возникает без специального волеизъявления лица: система фиксирует IP-адрес, время сессии, последовательность действий, технические ошибки, параметры устройства. В образовательной аналитике такие данные применяются для персонализации обучения и прогнозирования успешности [1]. В правовом споре они подтверждают или опровергают юридически значимые факты.

Первая особенность состоит в доказательственной асимметрии. Первичные данные хранятся у образовательной организации или оператора цифрового сервиса, а обучающийся обычно располагает только скриншотом, уведомлением, выгрузкой из личного кабинета либо копией отправленной работы. Поэтому спор о цифровом следе является не только спором о достоверности файла, но и спором о доступе к источнику данных. Локальные акты должны заранее определять, какие журналы событий ведутся, каков срок их хранения, кто формирует выгрузку и в какой форме обучающийся может запросить сведения о собственных действиях.

Вторая особенность связана с персональными данными. Цифровой след почти всегда позволяет прямо или косвенно идентифицировать лицо. При использовании прокторинга, записи

изображения, голоса, поведенческих характеристик и биометрической аутентификации уровень вмешательства в частную сферу возрастает. Следовательно, доказательственная полезность таких данных не отменяет требований законности, определенности цели обработки, минимизации состава собираемых сведений и информационной открытости для обучающегося.

Третья особенность проявляется при применении автоматизированных решений. Отчет системы прокторинга, антиплагиата или детектора использования генеративного искусственного интеллекта не должен механически подменять решение преподавателя, комиссии или суда. Алгоритмический вывод является производным цифровым материалом. Его сила зависит от возможности установить исходные данные, версию программного средства, критерии срабатывания, вероятность ошибки и порядок ручной перепроверки. Исследования политики ИИ в университетах также связывают допустимость таких инструментов с управлением рисками, приватностью и подотчетностью [2].

Для практического разрешения указанных проблем предлагается использовать паспорт образовательного цифрового следа. Это не новый вид доказательства, а форма описания цифрового материала при его представлении в комиссию по урегулированию спора, суд или иную компетентную инстанцию. В паспорте следует отражать источник сведений, образовательную программу или дисциплину, событие, дату и время, способ идентификации обучающегося, формат файла или загрузки, сведения о метаданных, лице, сформировавшем материал, сроках хранения, электронной подписи, хеш-значении либо иной контрольной отметке.

Отдельный блок паспорта должен быть посвящен правовому основанию обработки. Для обычных логов электронной образовательной среды достаточно указать связь с реализацией образовательной программы и локальным актом о применении электронного обучения. Для прокторинга, видеозаписи, голосовой фиксации и биометрической идентификации требуется более строгая проверка: был ли обучающийся заранее уведомлен, существовала ли менее инвазивная альтернатива, ограничен ли доступ к записи, установлен ли срок удаления, предусмотрен ли порядок обжалования результата. Такой подход согласуется с общей тенденцией к повышению требований к происхождению цифровых доказательств [3; 4].

Уровень проверки должен зависеть от риска. Низкий риск характерен для сведений о факте загрузки работы, подтвержденных журналом событий и уведомлением системы. Средний риск

возникает при споре о времени выполнения задания, количестве попыток тестирования или техническом сбое. Высокий риск имеется при обвинении в академической недобросовестности на основании прокторинга, антиплагиата или детектора ИИ. В последнем случае необходимы не только данные платформы, но и независимая перепроверка, участие комиссии, объяснения обучающегося и оценка совокупности доказательств.

Цифровой след обучающегося становится самостоятельным объектом правового внимания, поскольку соединяет доказательственную, образовательную и персонально-информационную функции. Его нельзя оценивать только по внешней форме файла или отчета платформы. Необходима проверка происхождения, целостности, принадлежности, правового основания обработки и возможности воспроизведения результата. Паспорт образовательного цифрового следа позволяет сделать такую проверку стандартизированной. Для образовательных организаций он может стать частью локального регламента электронного обучения и работы конфликтных комиссий, для обучающихся - средством доступа к данным, затрагивающим их образовательный статус, для суда - ориентиром при оценке цифровых доказательств. Наиболее строгие требования должны применяться к данным прокторинга и алгоритмическим выводам, поскольку именно они способны существенно повлиять на право лица продолжать обучение и получить документ об образовании.

Список литературы:

- [1] Шамсутдинова Т. М. Цифровой след как

источник больших данных (Big Data) в образовании // Открытое образование. - 2024. - № 6. - С. 13-21.

[2] Chan C. K. Y. A comprehensive AI policy education framework for university teaching and learning // International Journal of Educational Technology in Higher Education. - 2023. - Vol. 20. - Article 38.

[3] Казиханова С. С. Электронные доказательства в теории судебных доказательств // Digital Law Journal. - 2024. - Т. 5. - № 4. - С. 79-95.

[4] Ишеков К. А., Бокова Л. Н. Правовое регулирование использования информационных технологий в сфере образования // Конституционное и муниципальное право. - 2025. - № 1. - С. 45-48.

References:

[1] Shamsutdinova T. M. Digital footprint as a source of big data (Big Data) in education // Open education. - 2024. - № 6. - S. 13-21.

[2] Chan C. K. Y. A comprehensive AI policy education framework for university teaching and learning // International Journal of Educational Technology in Higher Education. - 2023. - Vol. 20. - Article 38.

[3] Kazikhanova S. S. Electronic evidence in the theory of forensic evidence // Digital Law Journal. - 2024. - VOL. 5. - № 4. - S. 79-95.

[4] Ishekov K. A., Bokova L. N. Legal regulation of the use of information technologies in the field of education // Constitutional and municipal law. - 2025. - № 1. - S. 45-48.

