ISSN 2949-1150 (online)
2071-8284 (print)

Научная статья
УДК 342.9

Опыт зарубежных юрисдикций по применению цифровых доказательств в административном процессе

Максим Геннадьевич Терехов

Всероссийский научно-исследовательский институт МВД России
Москва (121069, ул. Поварская, д. 25, стр. 1), Российская Федерация
Maxxx47@inbox.ru
https://orcid.org/0000-0002-2497-6329

Аннотация:
Введение. *В статье рассматривается опыт зарубежных юрисдикций в сфере применения цифровых доказательств в административном процессе. Анализируются правовые основы, практические аспекты и вызовы, связанные с использованием цифровых данных в качестве доказательств при рассмотрении дел об административных правонарушениях. Особое внимание уделяется проблемам обеспечения достоверности, целостности и допустимости цифровых доказательств, а также способам обеспечения справедливого и эффективного административного процесса как в национальной, так и в зарубежных юрисдикциях.*
Методология. *Сбор, обобщение, систематизация, сравнительный анализ теоретического материала и нормативных правовых актов, опрос и описание его результатов позволило всесторонне подойти к научному исследованию и достижению поставленной цели.*
По результатам исследования *сформулирован промежуточный вывод о том, что цифровые данные, применяемые в качестве нового вида доказательств, являются транснациональным явлением, имеющим схожие черты в правоприменительной практике зарубежных юрисдикций, требующим не только установления обособленного правового регулирования, но и совершенствования процессуального порядка их оборота. На основании существующего международного опыта с учетом особенностей отечественного административного права предложен авторский подход к этапам процессуальной работы с цифровыми данными, используемыми в качестве доказательств при производстве по делам об административных правонарушениях. При опросе ведущих специалистов и экспертов в области административного права и процесса на тему эффективности возможного законодательного дополнения подавляющее большинство респондентов высказались за необходимость закрепления процессуальных этапов работы с цифровыми доказательствами в Кодексе Российской Федерации об административных правонарушениях. Вместе с тем респонденты затруднились ответить на вопрос о форме возможного нормативного закрепления данной инициативы, что оставляет место для дальнейших научных дискуссий и развития заявленной темы исследования.*

Ключевые слова:
цифровые доказательства, административный процесс, электронные данные, национальная юрисдикция, достоверность, целостность, допустимость, цифровизация, производство по делам об административных правонарушениях

Для цитирования:
Терехов М. Г. Опыт зарубежных юрисдикций по применению цифровых доказательств в административном процессе // Вестник Санкт-Петербургского университета МВД России. 2026. № 1 (109). С. 57–67.

Статья поступила в редакцию 01.10.2025;
одобрена после рецензирования 12.12.2025;
принята к публикации 20.03.2026.

Original article

Foreign jurisdictions experience in the use of digital evidence in administrative proceedings

Maxim G. Terekhov

All-Russian Research Institute of the MIA of Russia
25, build. 1, Povarskaya str., Moscow, 121069, Russian Federation
Maxxx47@inbox.ru
https://orcid.org/0000-0002-2497-6329

Abstract:
Introduction. *The article examines the experience of foreign jurisdictions in the use of digital evidence in administrative proceedings. It analyses the legal frameworks, practical aspects and challenges associated with the use of digital data as evidence in the consideration of cases of administrative offences. Particular attention is paid to the problems of ensuring the reliability, integrity and admissibility of digital evidence, as well as ways to ensure a fair and effective administrative process in both national and foreign jurisdictions.*
Methodology. *The collection, generalisation, systematisation, comparative analysis of theoretical material and regulatory legal acts, survey and description of its results allowed for a comprehensive approach to scientific research and the achievement of the set goal.*
Based on the results *of the study, an interim conclusion was formulated that digital data used as a new type of evidence is a transnational phenomenon with similar features in the law enforcement practice of foreign jurisdictions, requiring not only the establishment of separate legal regulation, but also the improvement of the procedural order of its circulation. Based on existing international experience and taking into account the peculiarities of domestic administrative law, the author's approach to the stages of procedural work with digital data used as evidence in administrative offences proceedings is proposed. When leading specialists and experts in the field of administrative law and procedure were surveyed on the effectiveness of potential legislative amendments, the overwhelming majority of respondents expressed the need to codify the procedural stages of working with digital evidence in the Code of the Russian Federation on Administrative Offences. At the same time, respondents found it difficult to answer the question about the form of possible regulatory consolidation of this initiative, which leaves room for further scientific discussion and development of the stated research topic.*

Keywords:
digital evidence, administrative process, electronic data, national jurisdiction, reliability, integrity, admissibility, digitalisation, administrative offenses proceedings

For citation:
Terekhov M. G. Foreign jurisdictions experience in the use of digital evidence in administrative proceedings // Vestnik of Saint Petersburg University of the MIA of Russia. 2026. № 1 (109). P. 57–67.

The article was submitted October 1, 2025; approved after reviewing December 12, 2025; accepted for publication March 20, 2026.

Введение

На современном этапе развития общественных отношений мировая глобализация характеризуется нарастающим объемом цифровых технологий и их повсеместным проникновением во все сферы человеческой деятельности. Например, из анализа динамики статистических данных, опубликованных в отчете Международного союза электросвязи о развитии глобальной сети «Интернет», следует, что за 2024 год к сети «Интернет» было подключено 5,5 млрд человек, что на 227 млн человек больше, чем в 2023 году[1].

Тенденция, известная как цифровая трансформация или промышленная революция 4.0, оказывает масштабное влияние на все аспекты хозяйственной деятельности общества [1, с. 7–10], включая правовое регулирование, в т. ч. административно-правовое, являющееся одним из главных регуляторов, упорядочивающих общественные отношения.

Идут острые дискуссии ученых о позитивных и негативных эффектах цифровой трансформации общества, ее влиянии на изменение национальной правовой системы. В частности, В. В. Синюков, описывая проблематику легимитизации данных процессов, отмечает, что «соотношение правовой системы, системы права и социальной реальности делается гораздо более сложным»[2], и с таким утверждением следует согласиться.

С одной стороны, цифровые технологии открывают новые возможности для повышения эффективности государственного управления, оказания государственных услуг и взаимодействия с гражданами. Например, только за 2024 год в России цифровыми сервисами портала «Госуслуги» в сети «Интернет» воспользовались 750 млн раз. Одновременно с тем в цифровом виде на этом портале доступно более 200 массовых социально значимых федеральных и региональных услуг[3], что свидетельствует о массовой интеграции в государственное управление цифровых технологий, позволяющих решать проблему административных барьеров и бюрократизации государственных услуг для населения. М. В. Анисифорова отмечает: «Интернет по праву признается самым авангардным и, одновременно продолжающим набирать популярность инструментом» [2, с. 4].

[1] Глобальное число пользователей интернета растет, но неравенство сохраняется // Организация объединенных наций : [официальный сайт]. URL: https://news.un.org/ru/story/2024/11/1458816 (дата обращения: 25.08.2025).

[2] Цифровое право : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. Москва : Проспект, 2021. С. 16.

[3] Портал госуслуг занимает восьмое место по популярности среди всех российских интернет-сервисов // Информационное телеграфное агентство России (ИТАР-ТАСС) : [сайт]. URL: https://tass.ru/ekonomika/24588573 (дата обращения: 25.08.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

С другой стороны, цифровая трансформация порождает новые виды административных правонарушений, совершаемых в цифровой среде[4] или с использованием цифровых технологий. Кроме того, меняются способы фиксации административных правонарушений (согласно статистическим данным, только за 2024 год с помощью цифровых технологий было зафиксировано свыше 236,6 млн административных правонарушений, по итогам документирования которых были вынесены постановления на 149 млрд рублей[5]), тем самым обусловливая для науки необходимость переосмысления традиционных подходов к процессу доказывания и видам доказательств.

Все большее значение для административно-процессуальной деятельности приобретают новые виды информации, рассматриваемые наукой как «цифровые» и «электронные», активно применяемые на практике в соответствии со ст. 26.2 Кодекса Российской Федерации об административных правонарушениях[6] (далее– КоАП РФ), но не закрепленные законодательно как отдельный вид доказательств для КоАП РФ ввиду их специфики[7].

Общая потребность законодательного закрепления в главе 26 КоАП РФ понятия «электронных доказательств», что обосновывается в монографии М. В. Анисифоровой, Е. В. Машугиной и М. В. Андреяновым [3], по нашему мнению, утратила свою актуальность, поскольку большая часть информации, которая может быть отнесена к «электронным доказательствам» (электронные письма, сканированные документы, электронные договоры и т. д.), уже попадает под действие правил, установленных федеральными законами от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[8], от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[9] и другими нормативными актами, регулирующими электронный документооборот. В данных документах установлены требования к форме, порядку создания, хранения, передачи и юридической значимости электронных документов, что, по сути, уже задает определенные рамки для их применения в качестве доказательств при производстве по делам об административных правонарушениях. Если законодатель введет в КоАП РФ самостоятельное определение «электронных доказательств» и начнет устанавливать для них какие-то «особенные» процессуальные правила, отличные от тех, что действуют в сфере электронного документооборота, возникнет риск «дублирования» правового регулирования, что создаст дополнительную правовую путаницу и сложности для правоприменителей.

Целесообразно сосредоточиться на том, чтобы в КоАП РФ было четко определено понятие «цифровые доказательства», охватывающее весь спектр информации, полученной или созданной с использованием цифровых технологий, включая электронные документы, но не ограничиваясь ими. Это позволит учесть специфику новых видов цифровых данных, которые не вписываются в рамки традиционного электронного документооборота, и установить для них четкие правила применения в рамках административно-юрисдикционной деятельности при производстве по делам об административных правонарушениях. Например, к доказательствам такого рода относятся цифровые данные, воспроизведенные с помощью технологий искусственного интеллекта, интегрированных на камерах фото- и видеофиксации административных правонарушений в области безопасности дорожного движения в Российской Федерации.

[4] Цифровая среда – это правовая плоскость, в которой складываются общественные отношения посредством использования совокупности информационных технологий и (или) технологических устройств как в материальном мире, так и с альтернативной возможностью использования программного, технического взаимодействия в сети «Интернет» (См. подробнее: Терехов М. Г. Цифровое процессуальное право. Общая часть : учебное пособие. Москва : Проспект, 2025. С. 3–20 ; Его же. Цифровое право : учебное пособие. Москва : Блок-Принт, 202. С. 6–35).

[5] В России штрафы по камерам за нарушения ПДД составили более 149 млрд. рублей // Информационное телеграфное агентство России (ИТАР-ТАСС) : [сайт]. URL: https://tass.ru/ekonomika/23560889(дата обращения: 25.08.2025).

[6] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 31.07.2025) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2002. № 1 (ч. I). Ст. 1.

[7] Традиционное понятие доказательств в административном праве определяется как любые фактические данные, на основании которых уполномоченное должностное лицо устанавливает наличие либо отсутствие административного правонарушения, а также виновность лица в его совершении и иные обстоятельства, имеющие существенное значение для правильного разрешения дела в соответствии со ст. 26.2 КоАП РФ. Ключевым элементом данного определения является установление фактических данных. Следовательно, цифровые доказательства также должны соответствовать данному критерию, однако процесс установления и их оценки существенно отличается от работы с традиционными фактическими доказательствами. Цифровое доказательство можно определить как информацию (фактические данные), предоставленную в цифровой форме, полученную законным путем и имеющую значение для установления обстоятельств, подлежащих доказыванию в производстве по делам об административных правонарушениях.

[8] Об электронной подписи : Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 31.07.2025) // СЗ РФ. 2011. № 15. Ст. 2036.

[9] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 31.07.2025) // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

Следует также отметить, что перечень цифровых данных, которые могут применяться в качестве доказательств при производстве по делам об административных правонарушениях, не является исчерпывающим и имеет свои характерные признаки для их определения – цифровой формат (бестелесную форму).

Отсутствие законодательного закрепления отдельного вида доказательств, существующих в цифровой форме, при применении их в статусе доказательств при административном процессе сопряжено с рядом правоприменительных проблем, связанных с их оценкой на предмет достоверности, достаточности, относимости, допустимости и целостности (новый критерий, характерный для данного вида доказательств). В частности, возникает вопрос о том, как правоприменителю:

1) доказать, что электронное сообщение не было подделано;

2) обеспечить сохранность цифровых данных от несанкционированного доступа и изменений;

3) интерпретировать данные геолокации и другую сложную программно-техническую информацию в цифровой форме.

В связи с этим изучение и систематизация опыта зарубежных юрисдикций в сфере применения цифровых данных в качестве особого вида доказательств, требующего особого порядка административно-процессуальных действий, представляется актуальным и перспективным направлением научного исследования для последующего совершенствования административного законодательства и правоприменительной практики в условиях формирования новой среды правового регулирования[10].

Тем самым предопределяется *цель исследования* – формирование комплексного представления о законодательном опыте зарубежных юрисдикций по применению цифровых данных в качестве нового вида доказательств в административном процессе.

Методы

Сбор, обобщение, систематизация, сравнительный анализ теоретического материала и нормативно-правовых актов, опрос и описание его результатов позволили всесторонне подойти к научному исследованию и достижению поставленной цели.

Результаты

Общеизвестно, что одним из истоков и условий существования общества, государства во все времена является сохранение целостности его устоев, защита от явлений и деяний, которые представляют угрозу для этих устоев. Не случайно человечество с древнейших времен и по настоящее время стремится познать деструктивные явления и деяния, пытается минимизировать их опасность для общественных отношений. Как защитная реакция в ответ на нарушения условий жизни, в ней возникло нормирование поведения, установление государством санкций за неправомерные деяния. Развитие общественных отношений, расширение сферы административно-юрисдикционной деятельности, кодификация норм об административных правонарушениях в области цифровой среды обусловили в последние годы повышенное внимание науки и государственных структур к вопросам противодействия административной деликтности [4, с. 96].

К одной из центральных проблем развития института доказательств в административном праве, не получивших законодательного разрешения в настоящее время, как ранее уже отмечалось, следует отнести правоприменительную практику в отношении определения цифровых данных в качестве доказательств при производстве по делам об административных правонарушениях. В частности, М. В. Анисифорова, Е. В. Машугина и М. В. Андреянов, исследуя вопросы применения бестелесной формы доказательств (электронных доказательств), пишут, что «неполнота правовой регламентации, выражающаяся в отсутствии конкретного нормативного предписания о возможности применения электронных доказательств в юрисдикционном производстве, является существенным недостатком правового регулирования в этой сфере и противоречит общим целям охранительной деятельности, направленной на защиту прав и свобод человека и гражданина» [3, с.11].

В связи с этим изучение и систематизация правоприменительного и законодательного опыта, являющегося острием цифровой трансформации, в т. ч. в зарубежных странах, вызывает особый научный интерес.

[10] Цифровое право... С. 20.

ISSN 2949-1150 (online)
2071-8284 (print)

Впервые на международном уровне термин «цифровые доказательства» в развернутом виде официально упоминается в 2019 году в образовательных документах Организации Объединенных наций (далее – ООН), в частности, в «Образовательном модуле 4, Введение в цифровую криминалистику». Из смысла документа следует, что «цифровые отпечатки» являются следствием использования человеком информационно-телекоммуникационных технологий, а равно такие цифровые следы (активные и пассивные) могут быть использованы в качестве подтверждения или опровержения доказательства о факте совершения противоправных действий[11].

Примечательно, что образовательный материал ООН исходит из факта, что цифровые данные, используемые в качестве доказательств в административном и уголовном процессе, – не только заверенные электронной подписью документы в электронном виде, но и данные, которые хранятся в цифровых устройствах. Например, относительно цифровых данных хранящихся в компьютерах, смартфонах, планшетах, телефонах, принтерах, умных телевизорах и любых других устройствах, имеющих цифровую память, внешних запоминающих устройствах, сетевых компонентах и устройствах по типу серверов и облачных хранилищ данных[12].

Тем самым ООН декларирует для целей борьбы с противоправными явлениями свой понятийный аппарат на международном уровне, подчеркивая отсутствие исчерпывающего списка цифровых данных и уточняя, что необходимо руководствоваться общими признаками такого рода новых (цифровых) доказательств и общими процессуальными принципами.

Законодательный и правоприменительный опыт зарубежных юрисдикций в настоящее время не демонстрирует общей законодательной синергии на данный счет, позволяя выделить как схожие, так и отличительные черты в разрешении вопроса о процессуальном применении цифровых данных в качестве доказательств.

Для стран ближнего зарубежья включение цифровых данных в доказательственную базу по делам об административных правонарушениях стало неотъемлемой частью административного процесса. Однако этот процесс обусловил ряд значительных процессуальных проблем, связанных с определением правового статуса цифровых данных в качестве отдельного вида доказательств, обеспечением допустимости, достаточности, относимости и достоверности таких доказательств из-за отсутствия надлежащего правового регулирования.

Например, в статье 6.11 Процессуально-исполнительного кодекса Республики Беларусь об административных правонарушениях[13] «иные документы и другие носители информации», применяемые в качестве доказательств, включают перечень непроцессуальных носителей еще более широкий, нежели в КоАП РФ.

При этом, как и в России, в Белоруссии предъявляются весьма строгие нормативные требования к сертификации технических средств, используемых для фиксации административных правонарушений в различных сферах деятельности общества. В частности, данные, полученные со специализированных камер фото- и видеофиксации административных правонарушений, не прошедших обязательную техническую сертификацию, могут быть признаны недопустимыми доказательствами. Это ограничивает возможности использования цифровых данных, но одновременно повышает требования к их качеству и надежности, актуализируя в рамках союзного государства (России и Белоруссии) вопрос правового закрепления отдельного вида доказательств, в основе которых лежат цифровые фактические данные (цифровых доказательств).

Одновременно с тем статья 765 Кодекса Республики Казахстан об административных правонарушениях[14] закрепляет общие принципы доказывания, активно внедряются системы автоматической фиксации нарушений правил дорожного движения, такие как «Сергек». Однако возникают вопросы, касающиеся соблюдения прав граждан на защиту. В частности, граждане часто оспаривают штрафы, назначенные на основании данных «Сергек», ссылаясь на то, что не были уведомлены о ведении фото- и видеонаблюдения в конкретном месте.

Таким образом, законодательство и правоприменительная практика стран-участников Содружества Независимых Государств демонстрирует наличие схожих с Россией тенденций –

[11] Киберпреступность : Модуль 4 : Введение в цифровую криминалистику : учебный модуль. Вена : Организация Объединенных Наций, 2019. С. 5–6.

[12] Там же. С. 4.

[13] Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях от 6 января 2021 г. № 92-З (ред. от 10.01.2022) // Национальный правовой Интернет-портал Республики Беларусь : [сайт]. URL: https://pravo.by/document/?guid=11031&p0=HK2100092 (дата обращения: 25.08.2025).

[14] Кодекс Республики Казахстан об административных правонарушения от 5 июля 2014 года № 235-V (ред. от 10.01.2025) // Информационная система «Параграф» : [сайт]. URL: https://online.zakon.kz/Document/?doc_id=31577399&pos=14406;144#pos=14406;144 (дата обращения: 25.08.2025).

процессуальных и законодательных проблем, в частности, при подходах к применению цифровых доказательств в административном процессе и отсутствии их прямого закрепления в законе. Решение этих проблем требует совершенствования национального законодательства, что остается перспективой на ближайшие годы.

Европейские страны, принадлежащие к романо-германской правовой системе и исторически связанные с формированием отечественной системы права, характеризуются строгим подходом к определению цифровых данных в качестве нового вида доказательств. Суды отдают предпочтение четким законодательным нормам и формальным требованиям к доказыванию, опираясь на традиционный процессуальный порядок применения доказательств в производстве по делам об административных правонарушениях.

Так, германское административное право не содержит исчерпывающего перечня доказательств в цифровой форме, однако предусматриваются общие правила, когда суд вправе учитывать доказательства, имеющие значение для дела, в нематериальной форме, согласно абз. 2 § 2 Закона «Об административных процедурах»[15], где конкретизируется, что такими доказательствами могут быть электронные документы. Наглядным примером является решение Федерального административного суда по делу о незаконном распространении информации в сети «Интернет», в котором суд признал допустимым в качестве доказательства распечатку электронной переписки, заверенную нотариусом [6, с. 758].

Наряду с германским, французское административное право также не содержит четкого определения нового вида доказательств и их признаков, но имеет свою правоприменительную практику. Суды Франции ориентируются на общие принципы доказывания, в частности, на положения о письменных доказательствах и свидетельских показаниях. Допустимыми считаются цифровые данные, если они получены законным путем и подтверждают обстоятельства дела, включая электронные подписи, имеющие юридическую силу, равную собственноручной подписи.

В связи с этим более прогрессивными видятся нормы наднационального законодательства. Обращаясь к руководящим принципам, призванным облегчить использование и администрирование появления большого количества цифровых данных, которые возможно применять в качестве доказательств в административном процессе, странами Европейского Союза (далее – ЕС), Комитетом министров Совета Европы признается наличие нового вида доказательств – электронных доказательств[16] на межгосударственном уровне. Вместе с тем отмечается, что с электронными доказательствами неразрывно связан термин «метаданные», под которыми понимается электронная информация о других электронных данных, позволяющая идентифицировать, установить источник или проследить историю доказательства, а также соответствующие даты и время. Базовым инструментом для удостоверения метаданных служит электронная подпись[17].

Таким образом, в странах ЕС наряду с формализованным подходом в условиях масштабной цифровой трансформации всех сфер жизни особую роль играет электронный документооборот с соответствующим уровнем программно-технической защиты, а наличие неподтвержденных цифровых данных в административном процессе остается в серой правовой зоне для правосудия стран ЕС, в отличие от гражданского [8, с. 72] и уголовного законодательства, шагнувшего дальше в вопросах применения не только электронных документов, но и других цифровых данных, имеющих отношение к предмету разбирательства в качестве потенциального доказательства в данных странах.

Например, согласно ст. 706–796 Уголовно-процессуального закона Французской Республики[18] (Dessonorisationset des fixations d'images de certains lieux ou véhicules), во Франции развита система акустического и визуального наблюдения, применяемая сотрудниками полиции по решению суда, предполагающая применение аудио- и фотофиксации в транспортных средствах, жилых помещениях для установления информации, полученной из переговоров подозреваемого

[15] Закон «Об административных процедурах» от 25 мая 1976 г. (ред. от 18.07.2017) // Всемирная организация интеллектуальной собственности (ВОИС) : [сайт]. URL: https://www.wipo.int/wipolex/ru/legislation/details/16054 (дата обращения: 25.08.2025).

[16] Электронные доказательства – это любое доказательство, полученное на основе данных, содержащихся на каком-либо устройстве или созданных им, при этом функционирование такого устройства зависит от программного обеспечения или данных, хранящихся или переданных посредством компьютерной системы или сети (См. подробнее: Электронные доказательства в гражданском и административном судопроизводстве : Руководящие принципы Комитета министров Совета Европы 30 января 2019 и пояснительный меморандум. Страсбург : Совет Европы, 2019. С. 7).

[17] Там же.

[18] Уголовно-процессуальный кодекс от апреля 1958 г. (ред. от 13.08.2025) // ВОИС : [сайт]. URL: https://www.wipo.int/wipolex/ru/legislation/details/23231 (дата обращения: 25.08.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

с другими лицами[19]. В Австрии и Германии используют систему искусственного интеллекта, когда в ходе расследования преступлений применяется автоматизированный розыск по электронным архивам уголовных дел. Данные, содержащиеся в информационной базе о совершении преступлений, сравниваются со сведениями из других баз данных с целью установления подозреваемого в конкретном преступлении (ст. 98a Rasterfahndung (УПК ФРГ)[20]), ст. 141 Datenabgleich (УПК АР) [9, с. 78] и др.).

В отличие от континентальных стран, в Великобритании подход к определению цифровых данных, применяемых в качестве доказательств, более гибкий. Суды руководствуются прецедентным правом и принципами справедливости. Допустимыми считаются любые цифровые данные, если они имеют отношение к делу, достоверны и получены законным путем. Особый акцент в английской правоприменительной практике делается на оценке доказательственной силы цифровых данных в контексте конкретного дела.

Американская правовая система также характеризуется аналогично гибким подходом к определению и применению цифровых данных в качестве доказательств в каждом конкретном случае[21] и является фактически основоположником разработки процессуальных механизмов работы с электронными и цифровыми данными. В 2001 году была разработана первая методология по цифровой криминалистике “Digital Forensic Research Workchop”, основанная на протоколе Федерального бюро расследований США, для производства обыска на физическом месте преступления [10]. Это в последующем нашло свое отражение в ежегодном обновлении и усовершенствовании данной модели, а также формировании и развитии отдельного направления углубленной судебной экспертизы по вопросам исследования цифровых данных по делам о нарушении законов.

Федеральные правила доказывания США содержат специальные положения, регулирующие использование электронных записей и других видов цифровых данных в суде. Американские суды широко признают допустимыми такие доказательства, как электронная почта, текстовые сообщения, данные социальных сетей, записи с камер видеонаблюдения, данные геолокации и другие. Важным условием является соблюдение правил достоверности и допустимости исходя из этапов правильности процессуального закрепления.

Можно отметить, что за последние два десятилетия, несмотря на прецедентное право англо-саксонской системы права, характеризующейся всесторонним подходом к разбирательству в каждом конкретном деле, в США сформирована достаточно выверенная и апробированная процессуальная часть работы с цифровыми данными, которые могут быть использованы в качестве особого вида доказательств.

Особую научную ценность для учета эффективных законодательных и правоприменительных зарубежных практик представляет поэтапная процессуальная работа с цифровыми данными, используемыми в дальнейшем как доказательства [11; 12].

В связи с этим не утратило своей актуальности научное исследование в сфере цифровой криминалистики, проведенное американским ученым Gary Palmer, поэтапно описывающее порядок работы с цифровыми данными в рамках процессуальных действий [11].

К данным этапам следует отнести:

I этап – идентификация. Этап включает поиск и распознавание соответствующих доказательств, а также их документирование. На этом этапе приоритетные задачи сбора доказательств определяются на основе ценности и изменчивости доказательств.

---

[19] Головко Л. В., Гуценко К. Ф., Филимонов Б. А. Уголовный процесс в современных зарубежных государствах : учебное пособие. Москва : Зерцало-М, 2002. С. 71.

[20] Головенков П., Спица Н. Уголовно-процессуальный кодекс Федеративной Республики Германия – Strafprozessordnung (StPO) : Научно-практический комментарий и перевод текста закона. Potsdam : Universit□tsverlag Potsdam, 2012. С. 45.

[21] Примером может служить дело “Mosaid Technologies Inc. v. Samsung Electronics Co., Ltd.” (2005). В 2005 году федеральный судья Рональд Хеджес (федеральный окружной суд Округа Нью-Джерси) ввел санкцию в размере $ 566 838.00 против компании «Samsung Electronics Co.” и связанных с ней организаций за уничтожение электронной почты в деле о нарушении патента 44. Из материалов дела следует, что истец – компания “Mosaid Technologies” – требовал раскрытия электронных писем, связанных с вопросами нарушения патента, которые не были представлены ответчиком – компанией “Samsung”. Судья постановил, что компания “Samsung” была обязана сохранять и раскрывать электронные письма, хотя компания “Mosaid” прямо не перечисляла их в своем ходатайстве. Судья пришел к мнению, что «ни один разумный тяжущийся (reasonable litigant) не может поверить, что определение «документы» не включает в себя электронную почту». Компания “Samsung” и ее адвокаты в конечном итоге были вынуждены признать, что компания уничтожила электронные письма, связанные с этим делом. Вследствие этого, в дополнение к существенным денежным санкциям, судья указал, что присяжные заседатели будут проинформированы о том, что «ответчики не смогли раскрыть практически все технические и другие электронные письма по делу и что присяжным будет разрешено сделать вывод, что эти доказательства были бы неблагоприятными для ответчиков».

II этап – сбор. Этап предполагает сбор всех цифровых устройств, которые могут содержать данные, имеющие доказательную ценность. Эти устройства затем транспортируются в лабораторию судебной экспертизы или другое учреждение для сбора и анализа цифровых доказательств. На практике бывают случаи, когда сбор данных в статическом режиме является практически неосуществимым. В таких ситуациях осуществляется сбор данных в реальном времени. К примеру, системы критически важных объектов инфраструктуры (например, системы управления производственными процессами). Эти системы не могут быть отключены от питания, поскольку они предоставляют критически важные услуги. Поэтому в этих случаях осуществляется сбор данных в реальном времени, когда изменчивые и неизменяющиеся данные извлекаются из систем, работающих в реальном времени. Однако сбор данных в реальном времени может помешать нормальному функционированию систем управления производственными процессами (например, замедлять их работу).

III этап – получение. Цифровые доказательства необходимо получать без ущерба для целостности данных. Такое получение данных без их изменения осуществляется путем создания копии содержимого цифрового устройства (процесс, известный как «создание неискаженного образа»). Для того чтобы определить, является ли дубликат точной копией оригинала, значение хэш-функции рассчитывается с использованием математических вычислений; здесь для получения значения хэш-функции используется криптографическая хэш-функция. Если значения хэш-функции для оригинала и копии совпадают, то содержимое копии является точно таким же, что и в оригинале.

IV этап – сохранение. Целостность цифровых устройств и цифровых доказательств может быть обеспечена с использованием системы охраны доказательств. На данном этапе фиксируется исходная информация о том, кто осуществлял сбор доказательств, где и каким образом они были собраны, какие лица получили эти доказательства и когда они их получили.

V этап – анализ. Требует использования надлежащих инструментов и методов цифровой криминалистики для обнаружения цифровых данных.

Примечательным и вызывающим дополнительный научный интерес является отсутствие в правоприменительной практике США заключительного этапа, связанного непосредственно с процессуальным использованием цифровых данных в качестве доказательств, что может оказывать решающее действие на итоги административного процесса. Представляется, что одним из важнейших критериев применения такого рода доказательств является надлежащая квалификация правоприменителя, который должен иметь соответствующие знания в данной области, учитывать особенности характера цифровой формы информации и программно-технического порядка ее представления в административном процессе.

В Азии в качестве примера для изучения можно взять китайское административное право, которое находится в процессе активного развития и адаптации одной из ведущих в мире экономик к реалиям цифровой трансформации. Верховный суд Китая первым в мире учредил интернет-суд, который занимается разбирательством по делам, связанным с глобальной сетью, электронной коммерцией и авторскими правами в цифровой форме. Особенностью подобного рода юридического процесса является превалирующий вид цифровых данных, предоставляемых истцами и ответчиками в качестве доказательств при разбирательстве [13, с. 34]. Верховный суд Китая отмечает: «Суды, которые рассматривают дела, связанные с интернетом, должны признавать цифровые данные, представленные в качестве доказательств, при условии, что соответствующие стороны собирают и хранят эти данные в блокчейне с цифровыми подписями, надежными временными отметками, а также верификацией значения хэш-функций и могут подтвердить легитимность используемой технологии...»[22].

Китайские суды признают допустимыми цифровые данные, такие как электронная переписка, электронные документы, данные геолокации и другие. Важным условием является соблюдение правил проверки достоверности.

В свою очередь японское процессуальное законодательство, исторически подвергшееся влиянию как романо-германской, так и англосаксонской правовых систем, характеризуется более консервативным подходом к определению цифровых доказательств. Суды отдают предпочтение традиционным видам доказательств, таким как письменные документы и свидетельские показания. Однако цифровые данные также признаются допустимыми, если они получены законным путем и подтверждают обстоятельства дела. Особое внимание уделяется обеспечению достоверности и неизменности цифровых данных в качестве доказательств.

[22] Верховный суд Китая признал силу цифровых данных в качестве цифровых доказательств // Bits.media : Криптовалюты и блокчейн по-русски : [сайт]. URL: https://bits.media/verkhovnyy-sud-kitaya-priznal-yuridicheskuyu-silu-dokazatelstv-na-baze-blokcheyna (дата обращения: 25.08.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

В странах Африки практика применения цифровых доказательств в административном процессе находится на стадии становления. Законодательство в этой области развито слабо, а суды испытывают трудности с оценкой достоверности и надежности электронных данных.

Обсуждение

Законодательный и правоприменительный опыт зарубежных юрисдикций не является однородным и представляет сложность для интеграции в отечественное административное право и практику применения его норм.

При этом применение цифровых данных в качестве нового вида доказательств в административном процессе является неизбежной тенденцией во всем мире, обусловленной развитием цифровых технологий и общей цифровизацией жизни общества. Для эффективного развития российского законодательства в данной сфере необходимо учитывать как положительные, так и негативные аспекты зарубежного опыта.

Анализ правоприменительной практики и законодательного регулирования применения цифровых данных в качестве доказательств при производстве по делам об административных правонарушениях показывает, что отечественное административное право исторически испытывало сильное влияние зарубежной (романо-германской) правовой школы на формирование административного процесса. По этой причине наиболее схожие тенденции наблюдаются в странах ближнего зарубежья и Европы, относящихся к романо-германской правовой системе. Сходство обусловлено общими принципами доказывания, формализованным подходом к праву и акцентом на законность и обоснованность принимаемых решений. Вместе с тем существуют и отличия, связанные с особенностями национального законодательства и правовой культуры в вопросах правового оформления и организации процессуальных процедур.

Так, страны ЕС признают в административном процессе юридическую силу электронных доказательств, которые охватывают цифровые данные, подтвержденные электронной подписью. Вместе с тем в «серой» правовой зоне остаются иные цифровые данные, которые не признаются доказательствами и не могут быть приняты судами по логике проанализированных нормативных актов. В сравнении с отечественным административным процессом страны ЕС идут по более консервативному пути и являются менее прогрессивными в вопросах охвата перечня информации в цифровой форме, которая может быть признана доказательством. Схожим с отечественным остается подход правоприменителей к формальным требованиям к доказыванию и традиционному процессуальному порядку применения доказательств в производстве по делам об административных правонарушениях.

Исходя из опыта стран ЕС в исследуемом вопросе, а также в условиях прогрессивности отечественного правоприменения, для совершенствования административного права при выделении в отдельный вид цифровых доказательств, вероятно, потребуется законодательная оговорка или примечание о разграничении правового регулирования электронного документооборота и процессуального порядка работы с цифровыми данными, к которым могут быть отнесены в т. ч. электронные документы. Несмотря на различные мнения отечественных ученых, которые исследуют доказательства в цифровой форме как особый вид доказательств [14, с. 156], предполагается, что государством уделяется недостаточно внимания данному вопросу.

Вместе с тем за последние годы в США сформирована достаточно сильная, законодательно детализированная и апробированная процессуальная часть работы с цифровыми данными, которые могут быть использованы в качестве особого вида доказательств. Этому следует уделить особое внимание при развитии отечественного института доказательств, в частности, таким процессуальным этапам, как идентификация, сбор, получение, сохранение, анализ. Представляется необходимым дополнить этот перечень еще одним этапом – процессуальное применение. Это позволит гарантировать отсутствие подделки цифровых данных, обеспечить их сохранность от несанкционированного доступа и изменений, верно интерпретировать данные и другую сложную программно-техническую информацию в цифровой форме [15].

Опыт стран Африки и Азии в вопросах практики применения цифровых данных в качестве доказательств неоднозначен. Для развивающихся стран Африки вопрос законодательного регулирования цифровых данных в качестве доказательств находится на стадии становления, отсутствуют нормативное регулирование и правоприменительная практика. В странах Азии, например, в Китае, уровень правового регулирования высок, что обусловлено прогрессивным развитием цифровых технологий, цифровой грамотностью судей и законодательным регулированием, повышенным уровнем автоматизации правосудия, что для России представляется актуальным опытом для дальнейшего изучения.

В развитие сформулированной перспективной модели нормативного обособления цифровых доказательств от иных видов доказательств посредством дополнения главы 26 КоАП РФ новой статьей, касающейся процессуальных этапов работы с цифровыми доказательствами, на основе опыта зарубежных юрисдикций, с учетом проведенного анализа, а также выводов, сделанных в настоящей статье, был проведен опрос. В качестве респондентов, принявших участие в анкетировании, выступили 10 ведущих специалистов и экспертов в области административного права и процесса.

При постановке вопроса *об оценке необходимости закрепления процессуальных этапов работы с цифровыми доказательствами в КоАП РФ* большинство респондентов высказались о существующей потребности нормативного обособления цифровых доказательств. Один респондент затруднился ответить, отметив, что эффективность законодательной перспективы данного предложения под вопросом и требует более детального научно-правового анализа.

На вопрос о том, *насколько предложенный перечень этапов (идентификация, сбор, получение, сохранение, анализ, процессуальное применение) охватывает ключевые аспекты работы с цифровыми доказательствами при производстве по делам об административных правонарушениях*, большинство респондентов ответили, что в основном охватывает, но требует дополнений. Один респондент отметил частичный его охват.

По вопросу о том, *будет ли способствовать предлагаемая инициатива защите прав и законных интересов участников производства по делам об административных правонарушениях*, однозначного мнения у экспертов не сложилось.

Оценивая возможность практической реализации предлагаемых положений в текущих условиях, семь экспертов ответили, что они «реализуемы при существенных изменениях в практике и ресурсах», еще трое отметили, что инициатива не вызовет затруднений и может быть успешно внедрена при незначительных изменениях в практике.

Таким образом, большинство экспертов относят проблему правового регулирования цифровых доказательств в производстве по делам об административных правонарушениях к числу давно назревших и требующих разрешения. Вместе с тем отмечается перспектива предложенной модели нормативного обособления цифровых доказательств от иных видов доказательств посредством дополнения главы 26 КоАП РФ новой статьей о процессуальных этапах работы с цифровыми доказательствами.

Заключение

Подводя итог, можно заключить, что назрела потребность законодательного определения правовой природы цифровых доказательств как отдельного вида доказательств.

Статьи 26.2, 26.7 и 26.11 КоАП РФ оставляют широкое поле для усмотрения в вопросе допустимости и оценки цифровых данных, поскольку не обеспечивают достаточной правовой определенности.

Полагаем, что в КоАП РФ должно быть четко определено понятие «цифровые доказательства», охватывающее весь спектр информации, полученной или созданной с использованием цифровых технологий, включая электронные документы, но не ограничиваясь только ими. Это позволит учесть специфику новых видов цифровых данных, которые не вписываются в рамки традиционного электронного документооборота, и установить для них четкие правила применения в рамках административно-юрисдикционной деятельности при производстве по делам об административных правонарушениях.

В. В. Синюков отмечает: «Чтобы увидеть структурные процессы в праве, необходимо сделать технологии предметом правового регулирования на основе взаимодействия людей и объектов неживой природы»[23].

В связи с этим неотъемлемым элементом законодательной модернизации станет и административный процесс, определяющий процессуальные начала работы с цифровыми доказательствами. Особое место должно быть отведено опыту США по детализации и апробированию процессуальной части (этапам) работы с цифровыми данными, которые могут быть использованы в качестве особого вида доказательств. Это, в частности, рассмотренные в настоящей статье такие процессуальные этапы работы с цифровыми доказательствами, как идентификация, сбор, получение, сохранение, анализ и процессуальное применение. Этот опыт может стать основой для формирования собственного законодательства в данной сфере.

В перспективе именно благодаря опоре на зарубежный опыт российское административное право сможет укрепить внутреннюю согласованность, обрести технико-юридическую

[23] Цифровое право...

ISSN 2949-1150 (online)
2071-8284 (print)

устойчивость и выйти на уровень, соответствующий глобальной эволюции публичного правоприменения в цифровую эпоху. Существенную роль в развитии процессуальных начал применения цифровых данных в качестве самостоятельного вида доказательств (цифровых доказательств) будет играть накопленный США опыт, определивший за последние два десятилетия этапы процессуальной работы.

Список источников

1. *Шваб К.* Четвертая промышленная революция : [перевод с английского]. Москва : Эксмо, 2018. 285 с.

2. *Анисифорова М. В.* Административно-правовое обеспечение запрета пропаганды наркотиков в России и за рубежом : монография. Москва : Проспект, 2022. 312 с.

3. *Анисифорова М. В., Машугина Е. В., Андреянов М. В.* Теория и практика применения электронных доказательств в производстве по делам об административных правонарушениях : монография / науч. ред. А. П. Шергин. Москва : Инфра-М, 2020. 120 с.

4. *Шергин А. П.* Избранные научные труды / сост., предисл. А. С. Дугенец. Москва : Юрлит-информ, 2025. 399 с.

5. *Коровкин В. В.* Международное регулирование киберпространства: возможно ли эффективное взаимопонимание? // Социальные новации и социальные науки. 2020. № 1 (1). С. 60–76. https://doi.org/10.31249/snsn/2020.01.05

6. *Крамер У., Мицкевич Л. А., Васильева А. Ф.* Электронные формы в административном процессе России и Германии // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10, № 4. С. 756–780. https://doi.org/10.21638/spbu14.2019.410

7. *Верхелст Э., Ваутерс Я.* Глобальное управление в сфере кибербезопасности: взгляд с позиции международных прав и прав ЕС // Вестник международных организаций: образование, наука, новая экономика. 2020. Т. 15, № 2. С. 141–172. https://doi.org/10.17323/1996-7845-2020-02-07

8. *Гаврилов Е. В.* Скриншот как доказательство в арбитражном процессе // Арбитражные споры. 2020. № 2 (90). С. 75–92.

9. *Бутов В. Н.* Уголовный процесс Австрии : [монография]. Красноярск : Издательство Красноярского университета, 1988. 198 с.

10. *A Road Map for Digital Forensic Research* : By Collective work of all DFRWS attendees / From the proceedings of The Digital Forensic Research Conference DFRWS, 2001, USA Utica, NY (Aug 7th–8th). USA, New York : Utica, 2001. 42 p.

11. *Palmer G.* A Road Map for Digital Forensic Research : Technical Report (DTR-T001-01) for Digital Forensic Research Workshop (DFRWS). New York, 2001. P. 8–30.

12. *Kent R. [et al].* Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg : National Institute of Standards and Technology, 2006. 121 p.

13. *Галлямов Д. Р.* Интернет-правосудие: современный опыт Китая // Новый юридический вестник. 2023. № 1 (40). С. 34–36.

14. *Ермакова Е. П.* Цифровизация гражданского судопроизводства в США: закрепление процедуры электронного раскрытия доказательств («e-discovery») // Государство и право. 2022. № 11. С. 155–164. https://doi.org/10.31857/S102694520022769-6

15. *Научная школа профессора А. П. Шергина «Административная юрисдикция»* : монография / общ. ред. А. П. Шергина. Москва : ВНИИ МВД России, 2025. 162 с.

References

1. *Shvab K.* Chetvertaya promyshlennaya revolyuciya : [perevod s anglijskogo]. Moskva : Eksmo, 2018. 285 s.

2. *Anisiforova M. V.* Administrativno-pravovoe obespechenie zapreta propagandy narkotikov v Rossii i za rubezhom : monografiya. Moskva : Prospekt, 2022. 312 s.

3. *Anisiforova M. V., Mashugina E. V., Andreyanov M. V.* Teoriya i praktika primeneniya elektronnyh dokazatel'stv v proizvodstve po delam ob administrativnyh pravonarusheniyah : monografiya / nauch. red. A. P. Shergin. Moskva : Infra-M, 2020. 120 s.

4. *Shergin A. P.* Izbrannye nauchnye trudy / sost., predisl. A. S. Dugenec. Moskva : Yurlit-inform, 2025. 399 s.

5. *Korovkin V. V.* Mezhdunarodnoe regulirovanie kiberprostranstva: vozmozhno li effektivnoe vzaimoponimanie? // Social'nye novacii i social'nye nauki. 2020. № 1 (1). S. 60–76. https://doi.org/10.31249/snsn/2020.01.05

6. *Kramer U., Mickevich L. A., Vasil'eva A. F.* Elektronnye formy v administrativnom processe Rossii i Germanii // Vestnik Sankt-Peterburgskogo universiteta. Pravo. 2019. T. 10, № 4. S. 756–780. https://doi.org/10.21638/spbu14.2019.410

7. *Verhelst E., Vauters Ya.* Global'noe upravlenie v sfere kiberbezopasnosti: vzglyad s pozicii mezhdunarodnyh prav i prav ES // Vestnik mezhdunarodnyh organizacij: obrazovanie, nauka, novaya ekonomika. 2020. T. 15, № 2. S. 141–172. https://doi.org/10.17323/1996-7845-2020-02-07

8. *Gavrilov E. V.* Skrinshot kak dokazatel'stvo v arbitrazhnom processe // Arbitrazhnye spory. 2020. № 2 (90). S. 75–92.

9. *Butov V. N.* Ugolovnyj process Avstrii : [monografiya]. Krasnoyarsk : Izdatel'stvo Krasnoyarskogo universiteta,1988. 198 s.

10. *A Road Map for Digital Forensic Research* : By Collective work of all DFRWS attendees / From the proceedings of The Digital Forensic Research Conference DFRWS, 2001, USA Utica, NY (Aug 7th–8th). USA, New York: Utica, 2001. 42 p.

11. *Palmer G.* A Road Map for Digital Forensic Research : Technical Report (DTR-T001-01) for Digital Forensic Research Workshop (DFRWS). New York, 2001. P. 8–30.

12. *Kent R. [et al].* Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg : National Institute of Standards and Technology, 2006. 121 p.

13. *Gallyamov D. R.* Internet-pravosudie: sovremennyj opyt Kitaya // Novyj yuridicheskij vestnik. 2023. № 1 (40). S. 34–36.

14. *Ermakova E. P.* Cifrovizaciya grazhdanskogo sudoproizvodstva v SShA: zakreplenie procedury elektronnogo raskrytiya dokazatel'stv («e-discovery») // Gosudarstvo i pravo. 2022. № 11. S. 155–164. https://doi.org/10.31857/S102694520022769-6

15. *Nauchnaya shkola professora A. P. Shergina "Administrativnaya yurisdikciya"* : monografiya / obshch. red. A. P. Shergin. Moskva : VNII MVD Rossii, 2025. 162 s.