Научная статья
УДК 343.1
DOI: 10.47475/2311-696X-2026-50-3-57-61

С. 57–61

УНИВЕРСАЛЬНОСТЬ ПРЕДМЕТА ДОКАЗЫВАНИЯ (СТ. 73 УПК РФ) В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: ОТ ЦИФРОВЫХ СЛЕДОВ К ПРОГНОСТИЧЕСКИМ СИСТЕМАМ ИИ

Станислав Сергеевич Карабанов

Челябинский государственный университет, г. Челябинск, Россия
karabanov.stas@gmail.com

Аннотация. В статье анализируется нормативная конструкция предмета доказывания, закрепленная в ст. 73 Уголовно-процессуального кодекса Российской Федерации, где автор пытается определить ее универсальность и достаточность обусловленных цифровой трансформации уголовного процесса. Автор приходит к выводу, что перечень обстоятельств, подлежащих доказыванию (событие преступления, виновность, характер и размер вреда, обстоятельства, способствовавшие совершению преступления), в достаточной степени отражает особенности киберпреступлений и не нуждается в расширении за счет таких категорий, как «цифровой след», «электронное доказательство» или «предкриминальное поведение». Категория «пределы доказывания» также не утрачивает своего значения при работе с цифровыми следами и прогностическими системами искусственного интеллекта. Обосновывается позиция, согласно которой в условиях цифровой трансформации уголовно-процессуальных отношений отсутствует необходимость во внесении изменений или дополнений в ст. 73 УПК РФ.

Ключевые слова: предмет доказывания, пределы доказывания, ст. 73 УПК РФ, цифровая трансформация, цифровой след, искусственный интеллект, предкриминальное поведение, киберпреступления

Для цитирования: Карабанов С. С. Универсальность предмета доказывания (ст. 73 УПК РФ) в условиях цифровой трансформации: от цифровых следов к прогностическим системам ИИ // Правопорядок: история, теория, практика. 2026. № 3 (50). С. 57–61. DOI: 10.47475/2311-696X-2026-50-3-57-61

Research article

THE UNIVERSALITY OF THE SUBJECT OF PROOF (ARTICLE 73 OF THE CRIMINAL PROCEDURE CODE OF THE RUSSIAN FEDERATION) IN THE CONTEXT OF DIGITAL TRANSFORMATION: FROM DIGITAL TRACES TO PREDICTIVE AI SYSTEMS

Stanislav S. Karabanov

Chelyabinsk State University, Chelyabinsk, Russia
karabanov.stas@gmail.com

Abstract. The article analyzes the normative structure of the subject of proof enshrined in Article 73 of the Criminal Procedure Code of the Russian Federation in order to determine its universality and sufficiency in the context of digital transformation of criminal proceedings. The author concludes that the list of circumstances to be proved (the event of the crime, guilt, nature and extent of harm, circumstances contributing to the commission of the crime) fully covers the specifics of cybercrimes and does not require the inclusion of such categories as «digital trace», «electronic evidence» or «pre-criminal behavior» as independent elements of the subject of proof. The category of «limits of proof» also does not lose its significance when working with digital traces and predictive artificial intelligence systems. The article substantiates the position that Article 73 of the Criminal Procedure Code of the Russian Federation does not need to be amended or supplemented in connection with the digital transformation of social relations.

Keywords: subject of proof, limits of proof, Article 73 of the Criminal Procedure Code of the Russian Federation, digital transformation, digital trace, artificial intelligence, pre-criminal behavior, cybercrimes

For citation: Karabanov SS. Universality of the Subject of Proof (Article 73 of the Criminal Procedure Code of the Russian Federation) in the Context of Digital Transformation: from Digital Traces to Predictive AI Systems.

© Карабанов С. С.

Pravoporyadok: istoriya, teoriya, praktika [Legal and Order: History, Theory, Practice]. 2026;(3):57-61. (In Russ.). DOI: 10.47475/2311-696X-2026-50-3-57-61

Введение

Цифровая трансформация общественных отношений, активное внедрение информационно-телекоммуникационных технологий во все сферы жизни общества, а также экспоненциальный рост преступлений, совершаемых с использованием цифровых технологий, обостряют проблему готовности уголовно-процессуального законодательства к доказыванию по такого рода делам. По справедливому замечанию А. Б. Сергеева, практика расследования преступлений в сфере компьютерной информации значительно уступает по своей разработанности практике расследования «материальных» преступлений [12].

Материал и методы

В статье использованы нормативные правовые акты, регламентирующие вопросы уголовно-правовой ответственности за преступления совершаемые с использованием цифровых технологий, специальная литература по предмету исследования. Основу исследования составили общенаучные и частнонаучные методы научного познания, анализ теоретических и нормативных правовых источников, статистический, герменевтический методы.

Описание исследования

В юридической науке сформировались две полярные позиции относительно того, как институт доказывания должен реагировать на цифровые вызовы. Представители первой (условно «инновационной») позиции настаивают на необходимости кардинальной реорганизации всего уголовно-процессуального механизма судопроизводства, введении новых категорий («электронные доказательства», «цифровые доказательства») и даже разработке «цифрового доказательственного права» [7; 8]. Представители второй (условно «консервативной») позиции, к которой присоединяется и автор настоящей статьи, утверждают, что существующая теория доказательственного права универсальна и не требует изменений в связи с цифровой трансформацией [4; 12].

В рамках настоящей статьи предпринята попытка аргументированно доказать, что предмет доказывания, предусмотренный ст. 73 УПК РФ, является универсальной конструкцией, более чем достаточной для доказывания как по делам о так называемых компьютерных преступлениях, так и по делам, при расследовании которых используются или могут быть использованы прогностические системы искусственного интеллекта. При этом категория «пределы доказывания» также не утрачивает своего значения и не требует дублирующих положений.

Согласно концепции, изложенной в курсе уголовного процесса под редакцией Л. В. Головко, предмет доказывания является своего рода универсальной программой для следователя (дознавателя), определяющей границы поиска доказательств независимо от категории уголовного дела [5, с. 437]. Согласно ст. 73 УПК РФ, при производстве по уголовному делу подлежат доказыванию: 1) событие преступления (время, место, способ и другие обстоятельства совершения преступления); 2) виновность лица в совершении преступления, форма вины и мотивы; 3) обстоятельства, характеризующие личность обвиняемого; 4) характер и размер вреда, причиненного преступлением; 5) обстоятельства, исключающие преступность и наказуемость деяния; 6) обстоятельства, смягчающие и отягчающие наказание; 7) обстоятельства, которые могут повлечь освобождение от уголовной ответственности и наказания.

Важно подчеркнуть, что данный перечень является универсальным. Он не зависит от способа совершения преступления (материальный или цифровой), от его технической сложности или от новизны используемых преступником технологий. Событие преступления как центральный элемент предмета доказывания охватывает и неправомерный доступ к компьютерной информации (ст. 272 УК РФ), и создание вредоносных программ (ст. 273 УК РФ), и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ). Цифровой след — это не новое обстоятельство, подлежащее доказыванию, а предмет установления уже предусмотренных ст. 73 УПК РФ обстоятельств (времени, места, способа, виновности).

В диссертационном исследовании Д. С. Иванова обосновано отмечается, что предмет доказывания является универсальной информационной системой, объединяющий обвинительный и защитный компоненты, а его познание осуществляется через субъективную реальность, что предопределяет пределы доказывания [4, с. 44]. Данный подход представляется методологически верным, поскольку позволяет рассматривать предмет доказывания не как статичный перечень, а как динамичную систему, адаптируемую к специфике конкретного уголовного дела, в том числе совершенного в цифровой среде.

Исследуя философские (гносеологические) основания предмета доказывания, следует отметить, что познание явлений окружающей действительности лицами, осуществляющими деятельность по установлению виновности, происходит в известной степени через их субъективное восприятие реальности, что, в свою очередь, представляется особенно актуальным при работе с цифровыми следами, которые, в отличие от материальных, не имеют пространственной формы и воспринимаются опосредованно — через их отображение в цифровой информации.

© Карабанов С. С.

Физические особенности цифрового (электронно-цифрового) следа, как отмечает А. Г. Себякин, заключается в том, что он «означает след, зафиксированный в цифровых ЭВМ (компьютерных системах)», а его «информативность есть свойство содержащихся в нем компьютерных данных» [10, с. 12]. В отличие от материальных следов, изучаемых трасологией, цифровой след не имеет пространственной формы и возникает в результате изменения компьютерной информации (уничтожение, блокирование, модификация, копирование) [2, с. 3]. Однако это не требует изменения предмета доказывания. Как обосновано подчеркивается в криминалистической доктрине, трасологические закономерности, традиционно применяемые при работе с материальными следами, не могут быть экстраполированы на производство по уголовным делам о преступлениях в телекоммуникационном пространстве ввиду принципиально иной природы цифрового следа [12, с. 68]. Но это проблема не доказательственного права, а криминалистической тактики — методов обнаружения, фиксации и изъятия цифровых следов [12, с. 71].

В рамках существующей системы доказательств, в смысле ч. 2 ст. 74 УПК РФ, цифровая информация в полной мере согласуется с категориями вещественных доказательств (если информация хранится на материальном носителе, который сохранил следы преступного воздействия) или иных документов (если информация представлена в виде, пригодном для восприятия). Введение самостоятельной категории «электронные доказательства» не является необходимым. По справедливому замечанию Л. В. Головко, включение в систему доказательств самостоятельной категории «электронные доказательства» нарушит ее внутреннюю логику, поскольку цифровая информация в зависимости от формы фиксации уже относится к вещественным доказательствам либо к иным документам [3, с. 18; 10, с. 685].

В учебном пособии «Противодействие преступлениям в цифровом пространстве» отмечается, что «цифровое пространство — это совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и сайтов в сети Интернет и сетей связи» [9, с. 11]. При этом «место совершения преступления в цифровом пространстве предлагается определять как место ввода информации и выхода в информационную сеть с последующей реализацией из этого места преступного деяния» [9, с. 19]. Данный подход не нуждается в модификации предмета доказывания, поскольку установление места совершения преступления охватывается п. 1 ч. 1 ст. 73 УПК РФ («время, место, способ и другие обстоятельства совершения преступления»).

Отдельную и более сложную проблему представляет использование систем искусственного интеллекта для выявления предкриминального поведения и прогнозирования преступлений. Легальное определение искусственного интеллекта содержится в ст. 3 проекта № 1271570-8 Федерального закона «О поддержке развития технологий искусственного интеллекта в Российской Федерации», согласно которой «искусственный интеллект — комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их»[1].

С точки зрения текущих возможностей, которые дает ИИ, можно убедится, что уже сейчас применение таких систем позволяет получать результаты не уступающие по качеству своего содержания интеллектуальным продуктам человеческого интеллекта. Однако в контексте уголовно-процессуального доказывания возникает иной вопрос: могут ли результаты работы прогностических систем ИИ (выявление «предкриминального поведения») входить в предмет доказывания?

По нашему мнению, предкриминальное поведение следует рассматривать как совокупность социальных, экономических, организационных, психологических и иных факторов, создающих условия для формирования преступного умысла, подготовки или совершения преступления. Однако, согласно действующему УПК РФ, доказыванию подлежат только события, имевшие место в объективной реальности, а не прогнозы или предположения о возможном будущем поведении.

Согласно позиции О. И. Бойченко, достаточность доказательств выступает критерием, определяющим пределы доказывания: при наличии достаточной совокупности доказательств достигается достоверное знание, при их недостатке — лишь вероятное [1, с. 28]. Результаты ИИ-анализа предкриминального поведения по своей природе являются вероятностными (прогностическими). Включение их в предмет доказывания означало бы легализацию вероятного знания в качестве обстоятельства, подлежащего доказыванию, что противоречило бы презумпции невиновности (ст. 14 УПК РФ), поскольку доказыванию подлежат только факты, а не вероятности.

Следовательно, для нас представляется очевидным, что предмет доказывания не может включать в себя результаты ИИ-анализа предкриминального поведения. Также, такие результаты нельзя рассматривать как доказательства по уголовному делу. В свою очередь их использование как ориентирующей для следователя информации вполне обосновано в процессе осуществления действий, направленных на криминальную профилактику.

Кроме того, полагаем, что используемая законодателем категория «пределы доказывания» сохраняет свое значение и не требует модификации. Согласно доктринальным подходам, пределы доказывания охватывают, во-первых, границы познания обстоятельств

[1] Проект № 1271570-8 Федерального закона «О поддержке развития технологий искусственного интеллекта в Российской Федерации. URL: https://sozd.duma.gov.ru/bill/1271570-8 (дата обращения: 24.07.2026).

© Карабанов С. С.

дела (необходимость исследования фактов различных уровней), во-вторых, достаточный объем доказательств для достоверного установления каждого обстоятельства [5, с. 820].

Правильное определение пределов доказывания имеет важное практическое значение: оно позволяет, с одной стороны, минимизировать риск неполного установления обстоятельств, входящих в предмет доказывания, а с другой — избежать необоснованного расширения сферы поиска доказательств, что обеспечивает соблюдение принципа процессуальной экономии [1, с. 69].

Согласно позиции А. Р. Чикулиной, стандарт доказывания — это правовая методика, обеспечивающая формирование качественного знания как основания для стандарта доказанности; его реализация возможна лишь при наличии достаточной совокупности предмета и пределов доказывания [12, с. 11]. Данный подход применим и к цифровой среде: достаточность доказательств определяется не техническими особенностями их носителя, а их способностью достоверно установить обстоятельства, входящие в предмет доказывания.

При расследовании преступлений в сфере компьютерной информации следователь должен четко соотносить категории «предмет доказывания» (что доказывать) и «пределы доказывания» (каким объемом доказательств располагать). Использование прогностических систем ИИ не меняет сущности пределов доказывания. Алгоритмическая рекомендация не может служить основанием для расширения или сужения пределов доказывания. Следователь по-прежнему самостоятельно определяет, какие обстоятельства и в каком объеме необходимо установить, исходя из конкретной следственной ситуации и требований ст. 73, 74, 85–88 УПК РФ.

Заключение и вывод

Проведенный анализ позволяет сформулировать следующие выводы.

1. Предмет доказывания, предусмотренный ст. 73 УПК РФ, является универсальной нормативной конструкцией, не требующей изменений или дополнений в связи с цифровой трансформацией общественных отношений. В свою очередь, перечень обстоятельств, подлежащих доказыванию полностью охватывает специфику киберпреступлений.

2. Категории «цифровой след», «электронное доказательство» или «предкриминальное поведение» не нуждаются в выделении в качестве самостоятельных категорий в рамках предмета доказывания. Цифровой след — это не самостоятельное обстоятельство, а средство установления обстоятельств, предусмотренных ст. 73 УПК РФ. Что касается предкриминального поведения, полагаем, что оно также не входит в предмет доказывания, поскольку доказыванию подлежат только факты объективной реальности, а не прогнозы вероятностного характера.

3. Система доказательств (ч. 2 ст. 74 УПК РФ) достаточна для работы с цифровой информацией, которая может быть отнесена к вещественным доказательствам (при наличии материального носителя) или иным документам. Введение самостоятельной категории «электронные доказательства» не требуется и может привести к коллизиям в устоявшейся правовой доктрине.

4. Категория «пределы доказывания» не утрачивает своего значения при работе с цифровыми следами и прогностическими системами ИИ. Алгоритмические рекомендации не могут служить основанием для расширения или сужения пределов доказывания, а их использование не должно подменять процессуальную самостоятельность следователя (ст. 38 УПК РФ).

5. Ст. 73 УПК РФ не нуждается в изменении или дополнении в связи с цифровой трансформацией. Проблемы, возникающие при расследовании преступлений в сфере компьютерной информации, лежат в практической плоскости (недостаточная IT-квалификация следователей, типичные ошибки при изъятии цифровых следов) и должны решаться путем адаптации криминалистических методик, а не изменения доказательственного права [11].

Список источников

1. Бойченко О. И. Пределы доказывания по уголовным делам: дис. … канд. юрид. наук. Краснодар, 2017. 191 с.

2. Гаврилин Ю. В., Шипилов В. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 23. С. 2–5.

3. Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15–25. DOI: 10.24411/2414-3995-2019-10002

4. Иванов Д. С. Предмет и пределы доказывания при установлении фактических обстоятельств уголовного дела присяжными заседателями: дис. … канд. юрид. наук. Екатеринбург, 2025. 275 с.

5. Курс уголовного процесса / Под ред. д. ю.н., проф. Л. В. Головко. 2-е изд., испр. Москва, 2017. 1280 с.

6. Ложкин Ю. А. О некоторых вопросах собирания электронных доказательств в рамках предварительного расследования уголовных дел // Пермский юридический альманах. 2019. № 1. С. 678–686.

7. Обидин К. В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. № 11. С. 198–206. DOI: 10.17803/1994-1471.2020.120.11.198-206

8. Окоменко Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3. С. 120–124.

9. Противодействие преступлениям в цифровом пространстве: учебное пособие / под науч. ред. Е. В. Смахтина, Р. Д. Шарапова. Тюмень, 2023. 404 с.

© Карабанов С. С.

10. Себякин А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: автореф. дис. … канд. юрид. наук. Москва, 2021. 31 с.

11. Сергеев А. Б. Следственные действия и типичные ошибки при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2022b. № 3. С. 25–33. DOI: 10.18323/2220-7457-2022-3-25-33

12. Сергеев А. Б. «Цифровое» доказательственное право при производстве по уголовным делам о преступлениях в сфере компьютерной информации: вопросы целесообразности // Юридическая наука и правоохранительная практика. 2022. № 3 (61). С. 66–72.

13. Чикулина А. Р. Предмет и пределы доказывания при разрешении судом ходатайств об избрании мер пресечения: автореф. дис. … канд. юрид. наук. Челябинск, 2024. 23 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Карабанов Станислав Сергеевич

Старший преподаватель кафедры экономики отраслей и рынков, институт экономики отраслей, бизнеса и администрирования, Челябинский государственный университет (г. Челябинск, Россия).
E-mail: karabanov.stas@gmail.com

INFORMATION ABOUT THE AUTHOR

Stanislav S. Karabanov

Senior Lecturer at the Department of Economics of Industries and Markets, Institute of Economics of Industries, Business and Administration, Chelyabinsk State University (Chelyabinsk, Russia).
E-mail: karabanov.stas@gmail.com

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 12.08.2026.
Дата рецензирования статьи / Revised: 25.08.2026.
Дата принятия статьи к публикации / Accepted: 31.08.2026.

© Карабанов С. С.