

ЮРИДИЧЕСКИЕ НАУКИ

УДК 343

ПРОБЛЕМА ПРИМЕНЕНИЯ «ЭЛЕКТРОННЫХ» ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ

Валитова Виалина Ильгизовна, студент, специальность 40.05.02 Правоохранительная деятельность, Оренбургский государственный университет, Оренбург
e-mail: viiiial@icloud.com

Научный руководитель: **Никурадзе Наталья Олеговна**, кандидат юридических наук, доцент, доцент кафедры уголовного процесса и криминалистики, Оренбургский государственный университет, Оренбург
e-mail: nikinatali2012@yandex.ru

***Аннотация.** Актуальность темы обусловлена стремительной цифровизацией общества и возрастающей ролью электронных данных в уголовных делах, что требует совершенствования нормативной базы. Целью исследования является комплексное изучение применения «электронных» доказательств в уголовном процессе. В рамках исследования применялись диалектический, системный и статистический методы анализа, что позволило всесторонне оценить проблематику использования «электронных» доказательств. Основные результаты включают в себя выявление проблемных аспектов в данной области и предложение обоснованных путей их решения. Сформулированы авторские подходы к основным выводам и предложения по изменению действующего законодательства, автором дано определение и выявлены характерные признаки «электронных» доказательств. Результаты исследования могут иметь значение для совершенствования правовой базы, регулирующей расследование киберпреступлений, а также могут служить теоретической базой для последующих научных изысканий.*

***Ключевые слова:** уголовный процесс, «электронные» доказательства, киберпреступность, информационно-телекоммуникационные технологии, обнаружение, собирание «электронных» доказательств.*

***Для цитирования:** Валитова В. И. Проблема применения «электронных» доказательств в уголовном процессе // Шаг в науку. – 2025. – № 3. – С. 90–95.*

THE PROBLEM OF USING «ELECTRONIC» EVIDENCE IN CRIMINAL PROCEEDINGS

Valitova Vialina Ilgizovna, student, specialty 40.05.02 Law Enforcement, Orenburg State University, Orenburg
e-mail: viiiial@icloud.com

Research advisor: **Nikuradze Natalia Olegovna**, Candidate of Law, Associate Professor, Associate Professor of the Department of Criminal Procedure and Criminalistics, Orenburg State University, Orenburg
e-mail: nikinatali2012@yandex.ru

***Abstract.** The relevance of the topic is due to the rapid digitalization of society and the increasing role of electronic data in criminal cases, which requires improvement of the regulatory framework. The purpose of the study is a comprehensive study of the use of “electronic” evidence in criminal proceedings. The study used dialectical, systematic and statistical methods of analysis, which made it possible to comprehensively assess the problems of using “electronic” evidence. The main results include the identification of problematic aspects in this area and the proposal of reasonable ways to solve them. The author’s approaches to the main conclusions and proposals for changing the*



current legislation are formulated, the author defines and identifies the characteristic features of “electronic” evidence. The results of the study may be important for improving the legal framework governing the investigation of cybercrimes, and may also serve as a theoretical basis for subsequent scientific research.

Key words: criminal proceedings, «electronic» evidence, cybercrime, information and telecommunication technologies, detection, evaluation of «electronic» evidence.

Cite as: Valitova, V. I. (2025) [The problem of using «electronic» evidence in criminal proceedings]. *Shag v nauku* [Step into science]. Vol. 3, pp. 90–95.

Сегодня, в условиях цифровизации все стороны нашей жизни поглощаются цифровыми технологиями, повсеместно мы оставляем цифровые следы, которые могут свидетельствовать об обстоятельствах совершенного преступления. В настоящее время в уголовном процессе актуальна проблема использования доказательственной информации в электронной форме. Кроме того, рост преступности в киберпространстве увеличивается, но при этом правовое регулирование уголовно-процессуального законодательства существенно отстает от меняющихся общественных отношений.

Результаты исследования для Всемирного индекса киберпреступности (далее – WCI), обнародованные в 2024 году, чётко демонстрируют картину киберпреступности в различных государствах. Команда исследователей под руководством экспертов из Оксфордского университета в течение трёх лет разрабатывала первый в мире «Всемирный индекс киберпреступности». Согласно итогам WCI, Россия лидирует в списке стран по объёму киберпреступной деятельности на её территории¹. Разработчики индекса отметили, что анонимность киберпреступлений значительно затрудняла исследование, в котором приняли участие 92 эксперта.

В соответствии с официальными статистическими данными Министерства внутренних дел Российской Федерации по Оренбургской области² (далее – МВД России по Оренбургской области), за январь-февраль 2025 года на территории Оренбургской области зафиксировано 1 184 преступления, совершённые с использованием информационно-телекоммуникационных технологий (далее – ИКТ). Указанный показатель демонстрирует рост по сравнению с аналогичным периодом прошлого года (январь-февраль 2024): темп прироста составил 4%, что подтверждает устойчивую тенденцию к увеличению цифровой преступности.

Удельный вес преступлений, совершённых с использованием ИКТ, по отношению к общему числу зарегистрированных преступлений за аналогичный

период 2024 года, составил 43%, что свидетельствует о значительной цифровизации криминальной активности. Особенно тревожной представляется динамика тяжких и особо тяжких преступлений данной категории – их зарегистрировано 757, при этом темп прироста по сравнению с прошлым годом достиг 53,9%, а увеличение их удельного веса составило 42,3%. Это указывает на рост общественной опасности цифровых преступлений, всё чаще приобретающих квалифицирующие признаки высокой степени тяжести.

Статистика экономических преступлений, совершённых с использованием ИКТ, заслуживает особого внимания. Зафиксировано 43 таких преступления, что составляет 14,1% от общего числа экономических преступлений. При этом наблюдается значительный рост в 186,7%. Эти данные подчеркивают растущую уязвимость экономической сферы к киберпреступности и необходимость усиления мер по противодействию ей. Также зарегистрировано 14 преступлений, совершённых в особо крупном размере с ИКТ, что отражает значительный рост на 130% по сравнению с предыдущим периодом. Доля указанных преступлений в общей структуре преступности составляет 7,3%.

По преступлениям, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров или аналогов, сильнодействующих веществ, растений (либо их частей), содержащих наркотические вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ, зафиксирован резкий скачок: зарегистрировано 458 преступлений, демонстрирующих стремительный прирост на уровне 137,3% при увеличении удельного веса на 50,8%. Подобная динамика подтверждает тезис о том, что ИКТ становятся одним из ключевых инструментов в арсенале организованной преступности.

Заслуживает упоминания регистрация преступлений террористической направленности, совершённых с использованием ИКТ: за отчётный период на территории Оренбургской области выявлено два таких

¹ World Cybercrime Index (WCI) // Rau's IAS Study Circle. – URL: <https://compass.rauias.com/current-affairs/world-cybercrime-index/#::~text=Top%20Cybercrime%20Hotspots,are%20routed%20globally> (дата обращения: 19.03.2025).

² Данные о состоянии преступности в Российской Федерации за январь – февраль 2025 года. Отчет МВД России. – URL: <https://мвд.рф/> (дата обращения: 19.03.2025).

случая. Несмотря на скромное абсолютное значение, следует отметить 100-процентный прирост и аналогичное увеличение удельного веса. Это подчёркивает необходимость усиления киберпротиводействия угрозам экстремистского и террористического характера.

Следует уделить внимание неутешающей статистике общего количества нераскрытых преступлений прошлых лет, совершенных с использованием ИКТ на территории Оренбургской области по состоянию за январь-февраль 2025 года, которая составляет 24 193 случая. Зафиксирован прирост данного показателя на уровне 21,7%. Данные показатели свидетельствуют о необходимости усиления мер по противодействию киберпреступности и совершенствовании методик расследования преступлений, совершаемых в цифровой среде.

Таким образом, статистические данные МВД России по Оренбургской области за январь-февраль 2025 года свидетельствуют не только о количественном росте ИКТ-преступности, но и о её качественной трансформации – в сторону повышения степени организованности, тяжести и общественной опасности. Формирующийся тренд требует активного реагирования со стороны правоприменительных органов, совершенствования нормативного регулирования и модернизации методов цифровой криминалистики.

Исходя из вышеприведенной статистики, можно сделать вывод о том, что рост преступлений, совершенных с использованием ИКТ, увеличивается, вместе с тем возрастает потребность использования в доказывании по уголовным делам различных видов «электронных» доказательств (метаданные, IP-адреса, электронные носители, содержащие электронную информацию).

Специфика «электронных» доказательств, отличающая их от традиционных видов доказательств, порождает дискуссионные вопросы о важности законодательного закрепления понятия «электронные» доказательства, а также особенности собирания и оценки «электронных» доказательств. В теории уголовного права наблюдаются разногласия относительно необходимости формального определения термина «электронные» доказательства. По мнению А. А. Балашовой, в современных реалиях особое значение приобретают вещественные доказательства, связанные с электронными носителями и обладающие специфическими электронными характеристиками. Однако возникают трудности при попытке объединения термина «электронный» с понятием «доказательство» [1, с. 202]. Существует

и противоположное мнение П. С. Пастухова, в УПК РФ не следует вводить новый вид доказательства «электронное доказательство», необходимо лишь уточнить понятие «доказательство», указав, что сведения могут быть в виде электронной информации, которая, в свою очередь, «вполне способна восприниматься в одном из традиционных доказательств – вещественном доказательстве или документе» [6, с. 558–566]. Обобщая изложенное, можно заключить, что уголовно-процессуальное законодательство нуждается в совершенствовании в части закрепления понятия «электронные» доказательства.

Д. В. Замула отмечает, что «в настоящее время ни в одном нормативно-правовом акте не содержится понятие «электронное доказательство», а также нет законодательного закрепления того, какими признаками должно обладать такое доказательство для того, чтобы суд признал его допустимым и разрешил его использование в судебном процессе» [3, с. 189–191].

Нельзя не согласиться с мнением автора, поскольку совершенно неясно соответствует ли понятие термина «электронные» доказательства с предлагаемым законодателем в ч. 1 ст. 74 Уголовно-процессуального кодекса Российской Федерации³ (далее – УПК РФ) определению понятия доказательств в уголовном процессе. Значительные разногласия возникают при определении категории «электронных» доказательств: следует ли их классифицировать как вещественные доказательства или как иные документы? Введение четкого определения могло бы устранить эту неопределенность.

В противоположность вещественным доказательствам, электронные данные лишены осязаемой формы и не поддаются измерению стандартными физическими величинами. Ключевое значение имеет семантическое содержание информации, а не ее физическое воплощение. В отличие от этого, документ является продуктом человеческой деятельности, тогда как цифровая информация генерируется посредством алгоритмических процессов. Документы и вещественные доказательства воспринимаются сенсорной системой человека напрямую, в то время как для дешифровки цифровых данных необходима их интерпретация с использованием специализированного оборудования. Приоритет отдается смысловому содержанию, а не материальному носителю информации.

Так как, исследуемое нами понятие «электронные доказательства» не нашло свое отражение в ст. 5 УПК РФ, обратимся к ст. 2 Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных

³ Уголовный кодекс Российской Федерации: офиц. текст: по состоянию на 09 ноября 2024 г. // Собр. законодательства Рос. Федерации. – 2024 – № 46. – Ст. 6912.

технологиях и о защите информации»⁴, где закреплено определение электронного документа: «электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по ИКТ сетям или обработки в информационных системах» (ФЗ «Об информации, информационных технологиях и о защите информации»). Таким образом, определение электронного документа, представленное в ФЗ «Об информации, информационных технологиях и о защите информации», не решает вопрос о статусе электронных доказательств в уголовном процессе, что в очередной раз подчеркивает необходимость законодательного регулирования данной области.

Таким образом, сегодня понятие «электронные» доказательства является исключительно доктринальным и применяется для обозначения разного по объему массива технических новшеств.

В контексте рассматриваемой проблемы видится правильным рассмотреть уголовно-процессуальное регулирование данного вопроса в законодательстве зарубежных стран. Проведенный сравнительный анализ различных подходов к регулированию электронных доказательств может помочь выявить эффективные практики и механизмы, которые могут быть адаптированы или внедрены в законодательство.

Например, Уголовно-процессуальный кодекс Вьетнама (Criminal Procedure Code) (далее – УПК Вьетнама) в п. 1 ст. 87 выделяет источники доказательств, включая «электронные данные». Согласно ст. 99 УПК Вьетнама, электронные данные определяются как знаки, буквы, цифры, изображения, звук и аналогичные формы, которые создаются, хранятся, передаются, или их получают с помощью электронных средств [2, с. 86–88]. В рамках уголовного судопроизводства во Вьетнаме, согласно Уголовно-процессуальному кодексу, электронные данные признаются допустимым видом доказательств. Электронные данные, изначально находящиеся в электронных устройствах и системах, либо передаваемые или получаемые ими, при использовании совместимого программного обеспечения, проявляются в форме символов, числовых значений, визуальных представлений, аудиоматериалов или аналогичных форматов, доступных для человеческого восприятия (статья 95 УПК Вьетнама). Эти данные могут служить основанием для установления обстоятельств, имеющих значение для дела.

В частности, Уголовно-процессуальный кодекс Китайской Народной Республики может служить интересным примером, в котором ст. ст. 48, 50, 52, 54, 55 подчеркивают необходимость всестороннего, тщательного исследования всех доказательств, в том числе и электронных [8]. Также, электронные данные, представленные в форме файлов, переписок, изображений, видео- или аудиозаписей, могут быть отнесены к одному из этих видов доказательств (например, к документальным доказательствам или аудио- и видеозаписям) при условии соблюдения требований допустимости. Верховный народный суд КНР в своих разъяснениях и руководствах также дает толкование электронным доказательствам. В частности, к электронным доказательствам могут быть отнесены: данные электронной почты; сообщения в мессенджерах и социальных сетях; электронные документы; цифровые фотографии и видеозаписи; данные геолокации; история браузера и поисковых запросов; информация, хранящаяся на электронных носителях (компьютерах, смартфонах, серверах).

Таким образом, уголовно-процессуальное регулирование «электронных» доказательств в таких странах, как Вьетнам и Китай наглядно демонстрирует, что УПК Вьетнама четко определяет электронные данные как один из источников доказательств, что подчеркивает их важность в уголовном судопроизводстве, а УПК КНР осуществляет регулирование «электронных» доказательств через общие положения о доказательствах и через отдельные нормативные акты. Несмотря на отсутствие прямого определения, на практике под «электронными» доказательствами понимаются цифровые данные, которые могут быть использованы для установления обстоятельств уголовного дела. Приведенные прецеденты являют собой пример для адаптации продуктивных методик в иных юрисдикциях, стимулируя эволюцию в сфере применения «электронных» доказательств в уголовном судопроизводстве.

Принимая во внимание специфику «электронных» доказательств, целесообразно закрепить определение этого понятия на законодательном уровне. Это позволит избежать теоретических споров и перейти к актуальному правовому регулированию. Одним из возможных подходов к решению этой проблемы является внесение в ст. 5 УПК РФ следующей формулировки «электронного» доказательства: «электронные доказательства – это данные, хранящиеся на электронных и сетевых носителях, доступ к которым требует использования специальных электронных устройств,

⁴ Об информации, информационных технологиях и о защите информации: федер. закон № 149-ФЗ. // Собр. законодательства Рос. Федерации. – 2024. – № 48. – Ст. 7218.

признанные следователем релевантными, допустимыми и надежными».

Рассмотрев подходы к вопросу законодательного регулирования термина «электронные» доказательства и убедившись в самостоятельности данного понятия в контексте процессуального права, необходимо обратиться к проблеме – порядок собирания и оценки «электронных» доказательств. Она обладает определенной спецификой, которая, в свою очередь, обусловлена особенностями признаков этого вида доказательств. К числу таковых следует отнести: отсутствие материального выражения в о вещественной форме; подверженность изменчивости; высокий уровень риска уничтожения; фиксируются на определенных (магнитных – диски, серверы, флеш-накопители и др.) носителях; воспроизводятся только с помощью специальной техники и оборудования и с применением соответствующего программного обеспечения.

«Электронные» доказательства, равно как и доказательства в целом, могут быть получены посредством производства следственных и процессуальных действий. Наиболее часто используемыми в этих целях в судебно-следственной практике следственными действиями являются следственный осмотр, обыск и выемка. Уместно подчеркнуть, что результатом осуществления перечисленных следственных действий становится не обнаружение собственно доказательственной информации, а носителя ее хранения и обработки [7, с. 678–686].

Особенность фиксации электронных доказательств заключается в вариативности методов, используемых для этой цели. В частности, возможно изъятие физического носителя информации либо создание аутентичной копии данных на другой носитель, находящийся в распоряжении следственных органов. Следовательно, доступ к электронным следам реализуется путем их переноса на материальный носитель, обеспечивающий возможность дальнейшего исследования и использования в доказывании.

Собирание информации, хранящейся и обрабатываемой на удаленных серверах, представляет собой более сложную задачу, особенно если сервер расположен в другом субъекте РФ или за пределами страны. Данное обстоятельство в полной мере относится

и к облачным технологиям. В таких случаях, фиксация данных осуществляется посредством осмотра общедоступной информации, находящейся в открытом доступе [4, с. 20].

Для проведения следственных действий, направленных на собирание электронных доказательств, необходимо формирование специализированной следственно-оперативной группы, включающей экспертов в области информационных технологий. Это позволит зафиксировать максимальный объем информации, имеющей доказательственное значение, и повысить эффективность решения задач на начальном этапе расследования преступления [7, с. 102–118].

Оценка электронного доказательства на предмет допустимости предполагает установление законности его получения положениям УПК РФ. На настоящий момент не сформирована правовая база, определяющая порядок собирания, проверки и оценки «электронных» доказательств. Вследствие чего собственно процедура оценки этой разновидности доказательств во многом носит формальный, поверхностный характер. Кроме того, в судебно-следственной практике неоднозначно разрешается вопрос о законности производства осмотра телефона в целях извлечения из него переписки в отсутствие судебного решения. Спорным является вопрос об участии специалиста в ходе переноса (копирования) информации в рамках производства следственных действий.

В заключение, представляется целесообразным инкорпорировать в Уголовно-процессуальный кодекс понятие, предложенное нами ранее. Данный шаг позволит унифицировать терминологию и избежать разночтений при применении норм уголовно-процессуального права. Важно подчеркнуть, что не все электронные данные могут быть квалифицированы как «электронное» доказательство. Также видится правильным в ч. 2 ст. 74 УПК РФ определить «электронные» доказательства как еще один вид доказательств. Это позволит более четко регулировать их использование и оценку в процессе уголовного судопроизводства, а также поможет обеспечить правовую определенность и повысить эффективность работы с данными, хранящимися на электронных носителях.

Литература

1. Балашова А. А. К вопросу о понятии «Электронное доказательство» // Закон и право. – 2018. – № 6. – С. 120–122. – <https://doi.org/10.24411/2073-3313-2018-10031>.
2. Демидов Н. Н., Фам Ны Хан Проблемы, связанные со сбором и использованием электронных доказательств в уголовном деле во Вьетнаме // Закон и право. – 2021. – № 1. – С. 86–88. – <https://doi.org/10.24412/2073-3313-2021-1-86-88>.
3. Замула Д. В. Понятие электронных доказательств // Вестник современных исследований. – 2018. – № 8.4(23). – С. 189–191.

4. Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. – М. : Юрлитинформ, 2011. – 173 с.
5. Ложкин Ю. А. О некоторых вопросах собирания электронных доказательств в рамках предварительного расследования уголовных дел // Пермский юридический альманах. – 2019. – № 2. – С. 678–686.
6. Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // Седьмой Пермский конгресс ученых-юристов: Сборник научных статей, Пермь, 18–19 ноября 2016 года / Ответственные редакторы В. Г. Голубцов, О. А. Кузнецова. – Пермь: ООО «Издательство «СТАТУТ», 2017. – С. 558–566.
7. Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex Russica (Русский закон). – 2021. – Т. 74, № 9(178). – С. 102–118. – <https://doi.org/10.17803/1729-5920.2021.178.9.102-118>.
8. Уголовный кодекс Китайской Народной Республики / под общей ред. проф. А. И. Чучаева и проф. А. И. Коробеева, пер. с китайского проф. Хуан Даосю. 2-е изд. // ООО «ЮРИДИЧЕСКАЯ ФИРМА КОНТРАКТ». – 2021 – 312 с.

Статья поступила в редакцию: 13.05.2025; принята в печать: 02.07.2025.

Автор прочитал и одобрил окончательный вариант рукописи.