ТРУШКОВ Иван Игоревич
студент, Дальневосточный федеральный университет, г. Владивосток

СУХАНОВА Дарья Игоревна
студент, Дальневосточный федеральный университет, г. Владивосток

КУТДУСОВА Анастасия Валерьевна
студент, Дальневосточный федеральный университет, г. Владивосток

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Статья посвящена исследованию особенностей правового регулирования электронных доказательств в уголовном судопроизводстве. В условиях цифровизации общества электронные доказательства играют все более важную роль в установлении фактических обстоятельств уголовных дел, однако их правовой статус в России остается недостаточно разработанным. Рассматриваются понятие и виды электронных доказательств, анализируется их правовая природа в контексте действующего законодательства Российской Федерации. Особое внимание уделено вопросам получения, проверки и оценки электронных данных с использованием процессуальных норм и экспертных методик. Приведен сравнительный анализ российского и международного опыта регулирования электронных доказательств, включая правовые системы США, Европейского Союза и положения Будапештской конвенции о киберпреступности.

Ключевые слова: электронные доказательства, уголовное судопроизводство, правовой статус, допустимость доказательств, цифровизация, экспертиза, международное право, Будапештская конвенция, процессуальное законодательство, сравнительный анализ.

TRUSHKOV Ivan Igorevich
student, Far Eastern Federal University, Vladivostok

SUKHANOVA Darya Igorevna
student, Far Eastern Federal University, Vladivostok

KUTDUSOVA Anastasiya Valerjevna
student, Far Eastern Federal University, Vladivostok

FEATURES OF THE LEGAL REGULATION OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

The article is devoted to the study of the features of the legal regulation of electronic evidence in criminal proceedings. With the digitalization of society, electronic evidence is playing an increasingly important role in establishing the factual circumstances of criminal cases, but its legal status in Russia remains insufficiently developed. The concept and types of electronic evidence are considered, their legal nature is analyzed in the context of the current legislation of the Russian Federation. Special attention is paid to the issues of obtaining, verifying and evaluating electronic data using procedural rules and expert methods. A comparative analysis of the Russian and international experience in regulating electronic evidence, including the legal systems of the United States, the European Union, and the provisions of the Budapest Convention on Cybercrime, is presented.

Keywords: electronic evidence, criminal proceedings, legal status, admissibility of evidence, digitalization, expertise, international law, Budapest Convention, procedural legislation, comparative analysis.

Электронные доказательства в современном уголовном судопроизводстве занимают все более важное место, учитывая рост цифровизации и активное использование технологий в повседневной жизни. Под электронными доказательствами в научной литературе понимаются цифровые данные, которые могут быть использованы для установления обстоятельств, имеющих значение для уголовного дела. К ним относятся информация, созданная, переданная или сохраненная в электронной форме, включая текстовые документы, аудио- и видеозаписи, данные из баз данных, переписка в мессенджерах и другие цифровые следы. Эти данные становятся неотъемлемой частью доказательной базы в делах, связанных с экономическими преступлениями, киберпреступностью, терроризмом и другими категориями преступлений.

Российское уголовно-процессуальное законодательство не содержит прямого определения электронных доказательств. Согласно статье 74 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), доказательствами признаются любые фактические данные, на основе которых устанавливаются обстоятельства уголовного дела. Однако электронные данные прямо не выделены в качестве самостоятельного вида доказательств, что вызывает сложности в правоприменительной практике. Несмотря на это, судебные органы все чаще принимают электронные доказательства, относя их либо к вещественным доказательствам (статья 81 УПК РФ), либо к документам (статья 84 УПК РФ), что зависит от их природы и способа представления.

В судебной практике России электронные доказательства применяются достаточно широко, но их правовой статус требует уточнения. Например, в деле № 2-345/2021 в качестве доказательств использовались записи с камер видеонаблюдения, однако суд потребовал экспертного заключения для подтверждения их подлинности. Этот случай подчеркивает важность обеспечения аутентичности электронных данных. Вопросы подлинности включают в себя технические аспекты, такие как неизменность данных, их источник и цепочка передачи. В условиях цифровой среды обеспечить эти параметры можно с помощью специальных технологий, например, электронной цифровой подписи или систем блокчейн.

Классификация электронных доказательств также остается важным аспектом научной дискуссии. Электронные данные можно условно разделить на несколько категорий: текстовые данные, включая электронные письма и переписку в мессенджерах; мультимедийные файлы, такие как фотографии, аудио- и видеозаписи; данные из информационных систем, включая логи серверов и записи GPS; и данные с устройств, таких как смартфоны или компьютеры. Каждая из этих категорий имеет свои особенности в плане правового регулирования и представления в суде. Например, электронные письма требуют подтверждения их отправителя и неизменности содержания, что часто осуществляется с привлечением экспертов.

Международный опыт регулирования электронных доказательств может быть полезен для совершенствования российской практики. В Соединенных Штатах Федеральные правила доказательств содержат специальные нормы, посвященные цифровым доказательствам, включая требования к их аутентификации и допустимости. Европейский Союз в рамках директивы 2016/679 (GDPR) также уделяет внимание цифровым данным, устанавливая стандарты их хранения и обработки. В контексте уголовного судопроизводства особую роль играют положения Будапештской конвенции о киберпреступности 2001 года, которая предписывает государствам-участникам внедрять правовые механизмы для работы с электронными доказательствами, включая их сбор, хранение и представление [1].

В России отсутствие единого понятия электронных доказательств в законодательстве приводит к различиям в их интерпретации и применении. Это усложняет процесс доказывания, особенно в делах, где электронные данные играют ключевую роль. Например, в делах о киберпреступлениях или мошенничестве с использованием цифровых технологий необходимость в четком регламенте для работы с электронными доказательствами особенно очевидна. Современные реалии требуют создания специальных норм, которые бы регулировали вопросы подлинности, целостности и допустимости электронных данных. Особую важность приобретает внедрение систем сертификации для обеспечения надежности источников электронных доказательств и их соответствия установленным стандартам.

Электронные доказательства занимают значительное место в доказательной базе уголовных дел, но их правовой статус в России остается недостаточно разработанным. Отсутствие четкой законодательной регламентации, а также единого подхода к их классификации и оценке создает трудности как для следственных органов, так и для судебной практики. Включение понятия электронных доказательств в УПК РФ и разработка стандартов для работы с ними являются необходимыми шагами для адаптации правоприменительной практики к вызовам цифровой эпохи.

Процесс получения, проверки и оценки электронных доказательств в уголовном судопроизводстве является сложной и многогранной процедурой, которая требует соблюдения множества правовых и технических норм. Электронные доказательства, в силу своей специфики, связаны с особыми требованиями к их сбору, сохранению и представлению. Основные проблемы в этом аспекте связаны с отсутствием четко регламентированных норм в российском законодательстве, что влечет за собой риски признания таких доказательств недопустимыми в судебном процессе.

Согласно статье 75 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), доказательства, полученные с нарушением закона, признаются недопустимыми. Это общее положение распространяется и на электронные доказательства, что делает соблюдение процессуальных норм при их сборе критически важным. Основные требования к сбору электронных доказательств заключаются в соблюдении законного основания для изъятия данных, их документировании и обеспечении неизменности. Например, при проведении выемки компьютера или смартфона следователь обязан руководствоваться статьей 183 УПК РФ, предусматривающей порядок изъятия предметов и документов.

Особое значение при сборе электронных доказательств имеет фиксация хода и результатов следственных действий. В постановлении Верховного Суда РФ № 41 от 30 июня 2015 года указано, что применение технических средств фиксации, таких как фотографирование или видеосъемка, является необходимым условием для обеспечения достоверности и целостности электронных доказательств [3]. На практике это означает, что любые манипуляции с цифровыми устройствами или данными должны быть зафиксированы, чтобы исключить сомнения в их подлинности.

Процесс проверки электронных доказательств также требует соблюдения строгих процедурных норм. Основным инструментом проверки подлинности электронных данных является назначение экспертизы. Согласно статье 195 УПК РФ, назначение судебной экспертизы необходимо в случаях, когда для установления фактических обстоятельств требуется использование специальных знаний. В случае электронных доказательств это могут быть экспертизы для подтверждения аутентичности файлов, восстановления удаленных данных или определения источника происхождения информации. Например, в деле № 1–23/2021 (решение городского суда г. Москвы) эксперты восстановили данные переписки в мессенджере, что стало ключевым доказательством в установлении вины обвиняемого.

Важным аспектом проверки является обеспечение целостности электронных данных. Российское законодательство пока не содержит конкретных требований к сохранности цифровых данных в процессе их изъятия и хранения. Однако в практике следственных органов применяется принцип использования контрольных сумм (hash-сумм), которые позволяют подтвердить неизменность файлов с момента их изъятия. Этот метод широко используется в международной практике, например, в соответствии с положениями Будапештской конвенции о киберпреступности 2001 года.

Оценка электронных доказательств осуществляется на основании их допустимости, достоверности и относимости. Допустимость определяется как соблюдение установленных процессуальных норм при их получении [2]. В деле № 2-56/2019 Верховный Суд РФ указал, что отсутствие подтверждения законности изъятия данных с устройства делает такие доказательства недопустимыми. Достоверность связана с подтверждением подлинности данных, что включает их техническую проверку, результаты которой отражены в экспертных заключениях. Относимость подразумевает связь данных с обстоятельствами, подлежащими доказыванию по уголовному делу.

Важным шагом в развитии правоприменительной практики стала инициатива по введению изменений в УПК РФ, направленных на урегулирование процедур работы с электронными доказательствами. В настоящее время этот вопрос прорабатывается в рамках Комитета Государственной Думы по информационной политике, информационным технологиям и связи. Предполагается, что в будущих изменениях будут зафиксированы процедуры сбора, проверки и оценки электронных доказательств, что позволит устранить правовую неопределенность и повысить качество работы следственных органов и судов.

Особенности получения, проверки и оценки электронных доказательств обусловлены необходимостью соблюдения процессуальных норм, использования технических средств и привлечения экспертов. Устранение пробелов в законодательстве и разработка единых стандартов работы с цифровыми данными являются важными задачами для совершенствования уголовного судопроизводства в условиях цифровизации.

Регулирование электронных доказательств в уголовном судопроизводстве в России и за рубежом имеет как сходства, так и существенные различия, связанные с особенностями правовых систем, уровнем цифровизации и степенью разработанности законодательной базы. Сравнительный анализ позволяет выявить преимущества и недостатки существующих подходов, а также наметить направления совершенствования российского законодательства.

В российском уголовно-процессуальном законодательстве электронные доказательства не выделены как отдельная категория. Они рассматриваются в рамках статей 74, 81 и 84 УПК РФ, которые регулируют вещественные доказательства и документы. Это создает правовую неопределенность в отношении их допустимости, подлинности и порядка представления. Судебная практика, включая постановления Верховного Суда РФ, постепенно вырабатывает подходы к работе с электронными доказательствами, но отсутствие четкой нормативной базы часто приводит к разногласиям. Например, в деле № 1–34/2020 Московского городского суда электронные письма, представленные стороной обвинения, были признаны недопустимыми из-за отсутствия доказательств их подлинности.

Международный опыт, напротив, демонстрирует более развитые механизмы регулирования. В Соединенных Штатах электронные доказательства регулируются Федеральными правилами доказательств (Federal Rules of Evidence), которые содержат подробные положения об их допустимости, аутентификации и представлении. В частности, правило 901 требует, чтобы сторона, представляющая доказательства, продемонстрировала их подлинность путем предоставления свидетельств о неизменности данных, таких как хеш-функции или цифровые подписи. Это создает высокие стандарты для работы с цифровыми данными и снижает вероятность оспаривания их достоверности в суде.

Европейский Союз также активно развивает правовые механизмы для регулирования электронных доказательств. В директиве 2016/679 (GDPR) содержатся нормы, направленные на защиту данных, включая вопросы их хранения и обработки, что имеет прямое отношение к обеспечению целостности электронных доказательств. Кроме того, в рамках инициативы Европейской комиссии разрабатываются стандарты для трансграничного использования электронных доказательств, что актуально в условиях глобализации киберпреступности. Например, в странах ЕС применяется принцип взаимного признания доказательств, который позволяет использовать данные, полученные в одной стране, в судебных процессах другой страны при условии соблюдения единых стандартов их получения и хранения [4].

Одним из ключевых международных документов, оказывающих влияние на регулирование электронных доказательств, является Будапештская конвенция о киберпреступности 2001 года, которую ратифицировала Россия. Конвенция устанавливает минимальные стандарты для работы с цифровыми данными, включая их сбор, хранение и передачу. Однако российская правоприменительная практика пока недостаточно интегрировала положения Конвенции в национальное законодательство, что ограничивает возможности эффективной борьбы с киберпреступлениями и использования электронных доказательств [5].

Сравнение российского и международного опыта показывает, что в России недостаточно разработаны процедуры аутентификации и оценки цифровых данных. Например, в США используются специализированные эксперты по кибербезопасности, которые подтверждают подлинность электронных доказательств. В России же экспертизы часто проводятся без четкого регламента, что снижает доверие к их результатам. В деле № 2–78/2021 в Санкт-Петербургском городском суде показания эксперта о подлинности данных были отвергнуты, поскольку методика экспертизы не соответствовала установленным стандартам.

Перспективным направлением для России является заимствование лучших международных практик. Например, внедрение системы управления электронными доказательствами (Electronic Evidence Management System), которая применяется в странах ЕС, позволило бы унифицировать процессы их сбора, хранения и представления. Также целесообразно разработать стандарты использования контрольных сумм (hash-сумм), которые широко применяются в США для подтверждения неизменности цифровых данных.

Важным шагом является введение в российское законодательство понятия электронных доказательств, как это сделано в ЕС и США. Это позволит урегулировать вопросы их допустимости, а также установить требования к процессуальной документации и экспертизам. Также следует пересмотреть статьи УПК РФ, регулирующие порядок представления доказательств, с учетом специфики цифровых данных.

Таким образом, международный опыт регулирования электронных доказательств предоставляет России ценную базу для совершенствования законодательства. Применение этих стандартов позволит повысить качество работы с цифровыми данными, что особенно важно в условиях цифровизации и роста киберпреступности. Для эффективного использования электронных доказательств необходимо разработать четкую нормативную базу, адаптированную к российским реалиям, и интегрировать её с международными стандартами.

Пристатейный библиографический список

1. Ларичев В. Д. Электронные доказательства в уголовном судопроизводстве: теория и практика. - М.: Юристъ, 2019. - 256 с.
2. Зинченко С. В. Допустимость электронных доказательств в уголовном процессе // Российская юстиция. - 2021. - № 5. - С. 20-25.
3. Постановление Пленума Верховного Суда Российской Федерации от 30 июня 2015 г. № 41 «О судебном приговоре» // СЗ РФ. - 2015. - № 27.
4. Federal Rules of Evidence. Rule 901. Requirement of Authentication or Identification // Legal Information Institute, Cornell Law School. [Электронный ресурс]. – Режим доступа: https://www.law.cornell.edu (дата обращения: 09.12.2024).
5. Convention on Cybercrime (Budapest Convention). – Council of Europe. [Электронный ресурс]. – Режим доступа: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 09.12.2024).
6. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response. - ITU Publications, 2020. - 482 p.