DOI: 10.17803/1994-1471.2025.177.8.124-132

В. В. Платонов*

Обеспечение допустимости электронных доказательств в уголовном судопроизводстве

Аннотация. В статье обоснована необходимость конкретизации существующих в уголовно-процессуальной науке дефиниций понятия «электронное доказательство». Представлены результаты контент-анализа научной литературы, на основе которого выявлены виды критериев допустимости электронных доказательств в уголовном судопроизводстве и предложена их классификация. По итогам системного анализа уголовно-процессуального законодательства, правовых позиций Верховного Суда РФ, изучения уголовно-процессуальной практики, зарубежного опыта использования электронных доказательств в уголовно-процессуальном доказывании, эмпирического исследования, проведенного автором в 2024–2025 гг. в 12 субъектах РФ, актуализированы дополнительные критерии допустимости электронных уголовно-процессуальных доказательств, исходя из их цифрового происхождения и сферы существования. Предложено авторское определение электронного доказательства в уголовном судопроизводстве, систематизированы критерии его допустимости в целях оптимизации уголовно-процессуальной практики.

Ключевые слова: электронное доказательство; уголовное судопроизводство; критерии допустимости уголовно-процессуального доказательства; уголовно-процессуальное доказывание; уголовное дело; судебное обжалование; цифровизация; оценка электронных доказательств; достоверность электронного доказательства; фальсификация электронного доказательства.

Для цитирования: *Платонов В. В.* Обеспечение допустимости электронных доказательств в уголовном судопроизводстве // Актуальные проблемы российского права. — 2025. — Т. 20. — № 8. — С. 124–132. — DOI: 10.17803/1994-1471.2025.177.8.124-132.

Ensuring Admissibility of Electronic Evidence in Criminal Proceedings

Valentin V. Platonov, Postgraduate Student, Department of Criminal Procedure Law, Kutafin Moscow State Law University (MSAL), Lawyer, Moscow City Legal Consultation Bar Association, Moscow, Russian Federation
vvplatonov1994@yandex.ru

Abstract. The paper substantiates the need to clarify existing definitions of "electronic evidence" in criminal procedure science. Content analysis of scholarly literature reveals types and classifications of admissibility criteria for electronic evidence. Through a systematic analysis of criminal procedure legislation, legal positions of the Supreme Court of the Russian Federation, a study of criminal procedure practice, an empirical study conducted by the author in 2024-2025 in 12 constituent entities of the Russian Federation, and foreign experience in using electronic evidence in criminal procedure proving, additional criteria for the admissibility of electronic criminal

* *Платонов Валентин Васильевич*, аспирант кафедры уголовно-процессуального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), адвокат коллегии адвокатов «Московская городская юридическая консультация»
Садовая-Кудринская ул., д. 9, г. Москва, Российская Федерация, 125993
vvplatonov1994@yandex.ru

procedure evidence have been updated based on their digital origin and scope of existence. The author proposes a definition of electronic evidence in criminal proceedings, and systematizes the criteria for its admissibility in order to optimize criminal procedural practice.

Keywords: electronic evidence; criminal proceedings; admissibility criteria for criminal procedural evidence; criminal procedural proof; criminal case; judicial appeal; digitalization; evaluation of electronic evidence; reliability of electronic evidence; falsification of electronic evidence.

Cite as: Platonov VV. Ensuring Admissibility of Electronic Evidence in Criminal Proceedings. *Aktual'nye problemy rossijskogo prava*. 2025;20(8):124-132. (In Russ.). DOI: 10.17803/1994-1471.2025.177.8.124-132.

На современном этапе развития правового регулирования и уголовно-процессуальной практики распространено использование в качестве доказательств в уголовных делах электронных доказательств. Это напрямую связано с быстрым прогрессом в области информационных и коммуникационных технологий. Однако, несмотря на разработку многочисленных теоретических определений электронных доказательств процессуалистами, остается нерешенным вопрос конкретных критериев их допустимости в уголовном судопроизводстве. Данная проблема актуальна не только для российской, но и для международной юридической практики. Анализ законодательства европейских стран свидетельствует об отсутствии в большинстве случаев легальной дефиниции электронных доказательств, а также специальных правил признания их допустимыми.

Каждое доказательство в уголовном судопроизводстве, согласно ст. 75 УПК РФ, должно быть проверено на соответствие его допустимости. На необходимость конкретизации свойства допустимости электронных доказательств в уголовном судопроизводстве указывает О. В. Рябова, отмечающая «уникальность сферы появления и пребывания электронного доказательства, особый формат хранения рассматриваемого доказательства, предполагающий разнообразие объектов материального мира, использующихся для изъятия и последующего хранения электронного доказательства, обеспечение надежной сохранности в сравнении с бумажным носителем информации»[1].

В научной литературе встречается дефиниция критерия допустимости электронного доказательства: «правовое требование, определяющее соответствие полученного в ходе расследования уголовного дела электронного доказательства требованиям о надлежащем субъекте доказывания, источнике получения доказательственной информации, способе и процессуальной форме собирания доказательства, предусмотренных УПК РФ, соблюдении процедуры проверки доказательств, а также установление аутентичности, идентификации, верифицируемости и воспроизводимости электронной информации»[2].

В данной связи целесообразно акцентировать внимание на мнении Н. М. Кипниса, который выделил четыре критерия допустимости доказательства: «1) надлежащий субъект, правомочный проводить процессуальные действия, направленные на получение доказательств; 2) надлежащий источник фактических данных (сведений, информации), составляющих содержание доказательства; 3) надлежащее процессуальное действие, используемое для получения доказательств; 4) надлежащий порядок проведения процессуального действия (судебного или следственного), используемого как средство получения доказательств»[3].

---

1 *Рябова О. В.* Значение института «электронных доказательств» в отечественном уголовном судопроизводстве // Мировые исследования в области социально-гуманитарных наук : материалы III Международной научно-практической конференции. Рязань, 2023. С. 374–377.

2 *Количенко А. А.* Допустимость электронных доказательств в современном уголовном процессе // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 80–85.

3 *Кипнис Н. М.* Допустимость доказательств в уголовном судопроизводстве / отв. ред. П. А. Лупинская. М., 1995. С. 56.

Иные критерии допустимости электронных доказательств выделяются С. В. Зуевым: «1) аутентификация, 2) идентификация, 3) верифицируемость, 4) воспроизводимость сведений»[4].

Наряду с конкретизацией критериев допустимости уголовно-процессуальных электронных доказательств указанными учеными предлагается делить обозначенные критерии на общие и частные (аутентификация цифровой информации, идентификация цифровой информации). Указанная классификация критериев не снижает остроты дискуссии по поводу оптимальности отдельных элементов критериев допустимости электронных доказательств.

Следует подчеркнуть, что выделение данных вопросов обоснованно, т.к. неоднозначность решения при признании электронного доказательства допустимым обусловлена, с одной стороны, потребностью в поиске следов преступления и установлении обстоятельств, предусмотренных статьей 73 УПК РФ, а с другой стороны, необходимостью соблюдения конституционных прав личности, в отношении которой осуществляется уголовное преследование. Отмеченное подтверждается результатами изучения правоприменительной практики по рассмотрению судом жалоб заинтересованных лиц в порядке ст. 125 УПК РФ на нарушение тайны переписки при производстве осмотров электронных носителей в отсутствие судебных решений. Данная практика отражает наличие проблем, с которыми сталкиваются следователи, дознаватели при собирании, закреплении, оценке электронных доказательств, и указывает на необходимость совершенствования уголовно-процессуального законодательства в этой области.

Цифровая или электронная информация может храниться в любом из следующих источников: мэйнфреймы, сетевые серверы, персональные компьютеры, карманные устройства, автомобили или бытовая техника; в качестве альтернативы к ней можно получить доступ через облако, Интернет, частные сети или третьих лиц. Бóльшая часть такой информации создается и поддерживается в ходе обычной деятельности. Использование в уголовном судопроизводстве доказательственной информации, содержащейся в Интернете или на портативном устройстве, до сих пор не является единообразным. Анализ уголовно-процессуальной практики и мнений 78 респондентов из числа следователей СК России и МВД России, осуществляющих расследование преступлений в Москве, Санкт-Петербурге, Владимирской, Московской, Нижегородской, Новосибирской, Омской, Свердловской, Смоленской, Тверской, Тюменской, Ярославской областях, по вопросу оптимальности процессуального порядка применения электронных доказательств для установления обстоятельств, подлежащих доказыванию, показывает, что в правоприменительной деятельности распространено использование в качестве доказательств по уголовному делу скриншотов сообщений с телефона, распечаток переписок из социальных сетей, удаленных аудиосообщений, которые хранятся в памяти iPhone, переписок в приложении WhatsApp, электронных банковских выписок и т.д.

На актуальность вопроса надлежащей оценки анализируемых доказательств обращает внимание О. А. Малышева, отмечая «отсутствие четких критериев допустимости электронных доказательств в уголовном процессе, а также конкретных правил оценки электронных доказательств в ходе предварительного расследования»[5].

Оценка допустимости электронных доказательств в российском уголовном судопроизводстве часто опирается на прагматические сооб-

[4] *Зуев С. В.* О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 618–629.

[5] *Малышева О. А.* Трансформация досудебного уголовного производства в условиях цифровизации: тенденции и риски // Тенденции уголовной политики России на современном этапе развития общества : сборник статей Всероссийской научно-практической конференции, посвященной 25-летию кафедр уголовного права и криминологии, уголовного процесса и правоохранительной деятельности. Ижевск, 2024. С. 46–47.

ражения и не всегда осуществляется в строгом соответствии с уголовно-процессуальным законом, что ставит под сомнение допустимость таких доказательств. Это связано не столько с недостатком правового регулирования рассматриваемых уголовно-процессуальных отношений, сколько с недопониманием должностными лицами, осуществляющими предварительное расследование, правовой сущности электронных доказательств и их цифровой природы происхождения. Оценка допустимости доказательств в уголовном процессе требует проверки процедуры его получения в соответствии с уголовно-процессуальными нормами.

Научный интерес представляет позиция М. И. Воронина, определяющего условия признания допустимым доказательством такого электронного доказательства, как скриншот[6]. Подход ученого свидетельствует о том, что допустимость электронного доказательства связывается с участием лица, которое представляет его, а также с надлежащим порядком изъятия и приобщения доказательства к материалам уголовного дела. По нашему мнению, данная научная позиция свидетельствует о формальном подходе к приданию электронному доказательству свойства допустимости, т.к. в ней отсутствуют акцент на цифровом происхождении электронного доказательства и возможность внесения изменений в его содержание. Поэтому сложно поддержать мнение М. И. Воронина по исследуемому вопросу.

Наряду с изложенным существует и иная проблема в уголовном процессе — полноценное использование других (в бумажном формате) доказательств для подтверждения сведений, представленных в электронной форме. Анализ судебной практики свидетельствует о нередких случаях признания судами полученных в ходе предварительного расследования электронных доказательств допустимыми в тех случаях, когда их содержание подтверждается другими, неэлектронными доказательствами[7]. По мнению ряда ученых, «данный подход значительно ограничивает доказательственные возможности компьютерной информации»[8]. Однако с данной позицией осмелимся не согласиться, поскольку для признания электронного доказательства допустимым недостаточно только соблюдать процессуальную форму, установленный УПК РФ порядок изъятия и закрепления доказательства. По нашему мнению, акцент следует делать на цифровой природе происхождения и существования электронного доказательства, на которые выше обращалось внимание.

Современная уголовно-процессуальная практика оценки допустимости электронных доказательств часто характеризуется как произвольная, не учитывающая цифровое происхождение данного вида доказательства. Это связано в первую очередь с отсутствием системного нормативно-правового регулирования вопросов, касающихся собирания, проверки и оценки электронных доказательств. На необходимость оптимизации уголовно-процессуального законодательства в целях создания правовых условий надлежащего использования электронных доказательств при исследовании обстоятельств совершенного преступления указали 89 % респондентов. В частности, следователи отмечают: 1) действующее законодательство не позволяет применять электронные доказательства в доказывании по уголовным делам, исходя из их электронной природы; 2) требуется предусмотреть в законе отличные от традиционных способы собирания электронных доказательств.

Представляется, что в процессе собирания, проверки и оценки электронных доказательств

---

[6] *Воронин М. И.* Недопустимая допустимость электронных доказательств. Судебная практика и пробелы в УПК // Уголовный процесс. 2020. № 10. С. 46–55.

[7] Апелляционные определения Судебной коллегии по уголовным делам Верховного Суда РФ от 13.12.2018 по делу № 4-АПУ18-41 ; от 10.12.2019 по делу № 223-АПУ13-10 ; от 03.07.2013 по делу № 46-АПУ13-10 // СПС «КонсультантПлюс».

[8] *Титова К. А.*, *Литвинова И. В.* К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в российском уголовном процессе // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 2. С. 147.

необходимо предъявлять более строгие требования к электронной информации по сравнению с другими видами доказательств. Это связано с тем, что электронные данные неосязаемы, легко подвергаются изменениям и уничтожению и для их изучения требуются специальные средства и знания.

Если при использовании в доказывании электронных доказательств ограничиться исключительно традиционными критериями допустимости, что усматривается из судебных решений Верховного Суда РФ применительно к скриншотам, без выяснения происхождения и возможности внесения изменений в информацию, которая содержится на них, то возникает риск не заметить фальсификации электронных доказательств. Например, в ходе предварительного расследования следователями (дознавателями) осуществляется истребование сведений о соединениях между абонентскими устройствами, о банковских операциях. Организации запрашиваемую информацию предоставляют на электронных носителях, прилагаемых к ответам на запросы, не идентифицируя каким-либо образом содержимое. Анализ материалов уголовных дел показал, что предоставляемые сведения содержатся в текстовых файлах, допускающих внесение изменений (дополнение, удаление), которые влияют на объективное установление обстоятельств, предусмотренных статьей 73 УПК РФ. На практике по результатам производства осмотра предметов и документов содержимое текстового файла фиксируется в протоколе осмотра, в последующем признается вещественным доказательством и используется в доказывании по уголовному делу. Подобный порядок получения и закрепления электронного доказательства не обеспечивает объективного расследования уголовного дела и создает условия для фальсификации материалов уголовного дела. Поэтому представляется, что соблюдения лишь процессуального порядка, формы и т.д. недостаточно для электронного доказательства. При решении вопроса о допустимости электронных доказательств требуется учет дополнительных критериев. На данный факт указывает 77 % опрошенных в ходе эмпирического исследования.

Результаты изучения уголовно-процессуальной практики показывают, что к уголовным делам часто приобщаются скриншоты с различных интернет-сайтов, которые редактируются следователями, придерживающимися обвинительного уклона в доказательственной деятельности. Однако, т.к. подобные доказательства-скриншоты получены в установленном УПК РФ порядке, т.е. в ходе следственного действия и надлежащим должностным лицом, оформлены соответствующим протоколом, то по формальным основаниям они признаются допустимыми. При дальнейшем движении уголовного дела ни руководитель следственного органа, ни надзирающий прокурор не вникают в суть вопроса о допустимости этого электронного доказательства. Такая практика присуща и Верховному Суду РФ. Но нередко содержащаяся в них информация искажена. Возможности манипулирования электронными доказательствами разнообразны, и необходимо принять все возможные меры предосторожности против потенциальных изменений. Для этого, подвергая электронные доказательства критике и оцениванию, необходимо облегчить работу по определению их достоверности. Электронные доказательства должны использоваться в уголовном судопроизводстве только в том случае, если гарантируется, что доказательства на момент их применения соответствуют состоянию, в котором они были получены. Это направлено на предотвращение изменений доказательств в период между их получением и использованием в процессе доказывания. Кроме того, следует обеспечить, чтобы объем доказательств также не менялся в период между извлечением и использованием. Изложенное позволяет выделить еще один критерий допустимости электронных доказательств — защищенность от внешнего воздействия.

Обеспечение неизменяемости содержимого электронного доказательства позволит объективно устанавливать обстоятельства, предусмотренные статьей 73 УПК РФ. Простые распечатки электронных писем, мгновенных сообщений или комментариев в социальных сетях — это всего лишь репродукции, которые перед оспариванием можно исключить из понятия «электронные доказательства», если нет других спо-

собов подтверждения. По этой причине необходимо прибегнуть к экспертной проверке, например к сертификату, подтверждающему подлинность адреса электронной почты как средства доказательства, или к доверенному поставщику услуг, гарантирующему проверку электронной подписи на финансовом контракте. К числу средств, позволяющих обеспечить защищенность, следует отнести использование следователем, дознавателем электронно-цифровой подписи, шифрование, ограничение прав доступа к материалам уголовного дела. Электронная подпись является технологическим инструментом, позволяющим гарантировать подлинность и целостность электронных документов.

Для углубленного изучения представляет интерес «Унифицированная модель оценки допустимости цифровых доказательств», разработанная исследователями А. Антви-Боасиако и Х. Вентером[9]. Ученые акцентируют внимание на отдельных аспектах, которые касаются технических и юридических требований, имеющих существенное значение при определении допустимости электронных доказательств. Технические требования ориентированы на соответствие нормам в сфере работы с электронными доказательствами и их анализа, что основывается на знаниях, полученных в ходе научных исследований, правоприменительной практики и профессионального опыта в сфере digital forensics.

В частности, стандарты обращения с цифровыми доказательствами имеют значимую роль в процессе доказывания. В современных условиях интенсивного использования цифровых технологий в уголовном судопроизводстве актуализируется потребность в определении необходимых правил, регламентов и процедур использования электронных доказательств с учетом действующих норм. Отметим, что данный подход детализируется международным стандартом судебно-экспертной деятельности ISO/IEC 27037:2012, который может служить надежным руководством для допустимости электронных доказательств в правовой практике[10]. В документе подчеркивается, что его применение должно учитывать специфику национального законодательства и регулирования, не заменяя при этом законодательные требования какой-либо страны. Данный стандарт был создан в целях поддержки юридической значимости и усиления доказательственной силы электронных доказательств при расследовании и рассмотрении уголовных дел. В отечественном законодательстве необходимы минимальные стандарты безопасности данных. Требуется обеспечить, чтобы электронные доказательства не использовались в уголовном судопроизводстве, если нет достаточных доказательств того, что это не является результатом фальсификации или подделки документов. Для того чтобы проверить, соблюдены ли требования, не были ли электронные доказательства изменены с точки зрения определения содержания и объема информации в период между ее получением и использованием, а также не является ли она результатом фальсификации и подделки, важно иметь доступ к экспертным знаниям ИТ-специалистов. Необходимо обязать привлекать специалистов в области информационных технологий по просьбе подозреваемого или обвиняемого лица. Обратим внимание на тот факт, что в случае производства судебной экспертизы лицом, которое не имеет соответствующего допуска для ее производства, результаты экспертного исследования будут признаны недопустимым доказательством. Кроме того, в случае использования в ходе производства судебной экспертизы средств, у которых закончился срок действия лицензии, либо она отсутствовала или если эксперты не были приняты в подразделения, то полученное заключение эксперта невозможно будет признать допустимым. Поэтому соблюдение стандарта обращения с электронными доказательствами необходимо для обеспечения их допустимости в процессе доказывания.

[9] *Antwi-Boasiako A., Venter H*. A Model for Digital Evidence Admissibility Assessment // 13th IFIP International Conference on Digital Forensics (DigitalForensics), January 2017, Orlando, FL, United States. Springer, 2017. P. 23–38.

[10] URL: https://www.iso.org/standard/44381.html (дата обращения: 20.11.2024).

К числу правовых требований относят получение законного разрешения на производство следственного действия и изъятие электронных средств; подлинность полученной информации и относимость к обстоятельствам уголовного дела; сохранение исходного состояния и структуры цифровых данных; верификация (проверка) достоверности цифровой информации, под которой понимается отсутствие сомнений по каждому из критериев надежности цифровых доказательств[11].

Кроме того, представляют интерес правовая регламентация допустимости электронных доказательств и правоприменительная практика в Индии. В частности, разделы 65A и 65B Закона о доказательствах 1872 г. касаются информации, содержащейся в электронных записях[12]. Согласно примечанию к разд. 65A в этой норме изложены «специальные положения» относительно доказательств, касающихся электронных записей. Примечание к разд. 65B затем ссылается на «допустимость электронных записей», предусматривающую, что если какая-либо информация, содержащаяся в электронной записи, созданной с помощью компьютера, была скопирована на оптический или магнитный носитель, то такая скопированная электронная запись «также считается документом» при соответствии условиям, изложенным в разд. 65B(2). Раздел 65B(2) предусматривает некоторые условия, которые должны быть соблюдены для принятия электронных записей в качестве доказательств: компьютер использовался лицом для хранения или обработки информации для осуществления какой-либо деятельности на регулярной основе в течение определенного времени, и лицо имеет законный контроль над использованием компьютера; такая информация должна была регулярно вводиться в компьютер в ходе обычной деятельности. На протяжении всего указанного периода компьютер работал исправно, и даже если нет, это не влияет на электронную запись или точность его содержания и информации в электронной записи, воспроизведенной/полученной из информации, введенной в компьютер в ходе обычной деятельности.

В деле «Anvar P.V. v. P.K. Basheer and ors.» суд истолковал разд. 22A, 45A, 59, 65A и 65B индийского Закона о доказательствах и постановил, что вторичные данные, содержащиеся на CD, DVD или флеш-накопителе, недопустимы без сертификата в соответствии с разд. 65B(4) данного Закона. В этом деле было указано, что электронные доказательства без сертификата в соответствии с разд. 65B не могут быть подтверждены устными доказательствами, а также мнение эксперта в соответствии с разд. 45A упомянутого Закона не может быть использовано для того, чтобы сделать такие электронные доказательства допустимыми. После этого дела было разъяснено, что единственный способ доказать электронную запись — это представить оригинальный носитель в качестве первичного доказательства и его копию в качестве вторичного доказательства в соответствии с разд. 65B индийского Закона о доказательствах. После этого Верховный суд в деле Шафхи Мохаммада постановил, что требование о представлении сертификата, в соответствии с разд. 65B(4), является процессуальным и не всегда обязательно. Сторона, не владеющая устройством, с которого был получен документ, не может быть обязана представить сертификат в соответствии с разд. 65B(4). Суд счел, что процессуальное требование, в соответствии с разд. 65B(4), должно применяться только в том случае, если электронное доказательство представлено лицом, контролирующим указанное устройство и, следовательно, имеющим возможность представить такой сертификат. Однако, если лицо не владеет устройством, разделы 63 и 65 не могут быть исключены[13].

[11] *Goodison S. E., Davis R. C., Jackson B. A.* Digital Evidence and the U. S. Criminal Justice System // URL: https://www.rand.org/pubs/research_reports/RR890.html (дата обращения: 20.11.2024).

[12] Indian Evidence Act, 1872 // URL: https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf (дата обращения: 20.11.2024).

[13] The Admissibility of Electronic Evidence // URL: https://www.foxmandal.in/the-admissibility-of-electronic-evidence/ (дата обращения: 20.11.2024).

Анализ представленного зарубежного опыта свидетельствует о целесообразности обогащения российской теории уголовно-процессуального доказывания классификацией критериев (требований) допустимости электронных доказательств, подтверждает необходимость обязательного участия специалиста при получении электронного доказательства в целях соблюдения технических условий, предусмотренных стандартами обращения с электронными доказательствами и их исследования. При привлечении специалиста для собирания электронных доказательств следователь, дознаватель не должны ограничиваться формальным участием первого в следственном действии в виде присутствия и фиксации данных в протоколе следственного действия. В данном случае действия специалиста должны быть направлены на получение электронного доказательства в целостном, неизмененном виде.

Таким образом, с учетом анализа научных позиций ученых, результатов эмпирического исследования допустимость электронных доказательств в уголовном судопроизводстве следует трактовать как требование, определяющее соответствие полученного в ходе уголовного судопроизводства доказательства предписаниям о надлежащем субъекте доказывания, об источнике получения доказательственной информации, предусмотренном в ст. 74 УПК РФ, о способе и процессуальной форме собирания доказательств, установленных УПК РФ, а также отвечающее критериям: аутентичности, идентификации, целостности, достоверности, воспроизводимости электронной информации, ее защищенности, обеспечивающее соблюдение стандартов обращения с электронными доказательствами.

Необходимость определения дополнительных критериев допустимости электронных доказательств в отечественном уголовном судопроизводстве обусловлена тем, что конституционные права граждан наиболее подвержены ограничению в уголовном процессе. Как следствие, использование электронных доказательств при расследовании и рассмотрении уголовного дела должно сопровождаться установлением надежных средств минимизации рисков незаконного и необоснованного нарушения прав, законных интересов личности, вовлеченной в уголовное судопроизводство, при этом не препятствующих эффективному доказыванию по уголовному делу в условиях цифровизации общественных отношений.

БИБЛИОГРАФИЯ

1. *Воронин М. И.* Недопустимая допустимость электронных доказательств. Судебная практика и пробелы в УПК // Уголовный процесс. — 2020. — № 10. — С. 46–55.
2. *Зуев С. В.* О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. — 2019. — № 2. — С. 618–629.
3. *Кипнис Н. М.* Допустимость доказательств в уголовном судопроизводстве / отв. ред. П. А. Лупинская. — М., 1995. — 128 с.
4. *Количенко А. А.* Допустимость электронных доказательств в современном уголовном процессе // Вестник Санкт-Петербургского университета МВД России. — 2022. — № 3 (95). — С. 80–85.
5. *Малышева О. А.* Трансформация досудебного уголовного производства в условиях цифровизации: тенденции и риски // Тенденции уголовной политики России на современном этапе развития общества : сборник статей Всероссийской научно-практической конференции, посвященной 25-летию кафедр уголовного права и криминологии, уголовного процесса и правоохранительной деятельности. — Ижевск, 2024. — С. 43–50.
6. *Рябова О. В.* Значение института «электронных доказательств» в отечественном уголовном судопроизводстве // Мировые исследования в области социально-гуманитарных наук : материалы III Международной научно-практической конференции. — Рязань, 2023. — С. 374–377.

7. *Титова К. А., Литвинова И. В.* К вопросу о возможности применения существующих критериев допустимости доказательств к электронным доказательствам в российском уголовном процессе // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. — 2022. — № 2. — С. 144–152.
8. *Antwi-Boasiako A., Venter H*. A Model for Digital Evidence Admissibility Assessment // 13th IFIP International Conference on Digital Forensics (DigitalForensics), January 2017, Orlando, FL, United States. — Springer, 2017.
9. *Goodison S. E., Davis R. C., Jackson B. A*. Digital Evidence and the U. S. Criminal Justice System // URL: https://www.rand.org/pubs/research_reports/RR890.html.
10. The Admissibility of Electronic Evidence // URL: https://www.foxmandal.in/the-admissibility-of-electronic-evidence/.

Материал поступил в редакцию 10 февраля 2025 г.

REFERENCES (TRANSLITERATION)

1. Voronin M. I. Nedopustimaya dopustimost elektronnykh dokazatelstv. Sudebnaya praktika i probely v UPK // Ugolovnyy protsess. — 2020. — № 10. — S. 46–55.
2. Zuev S. V. O sovremennoy kontseptsii razvitiya informatsionnykh tekhnologiy v ugolovnom sudoproizvodstve (RITVUS) // Permskiy yuridicheskiy almanakh. — 2019. — № 2. — S. 618–629.
3. Kipnis N. M. Dopustimost dokazatelstv v ugolovnom sudoproizvodstve / otv. red. P. A. Lupinskaya. — M., 1995. — 128 s.
4. Kolichenko A. A. Dopustimost elektronnykh dokazatelstv v sovremennom ugolovnom protsesse // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. — 2022. — № 3 (95). — S. 80–85.
5. Malysheva O. A. Transformatsiya dosudebnogo ugolovnogo proizvodstva v usloviyakh tsifrovizatsii: tendentsii i riski // Tendentsii ugolovnoy politiki Rossii na sovremennom etape razvitiya obshchestva: sbornik statey Vserossiyskoy nauchno-prakticheskoy konferentsii, posvyashchennoy 25-letiyu kafedr ugolovnogo prava i kriminologii, ugolovnogo protsessa i pravookhranitelnoy deyatelnosti. — Izhevsk, 2024. — S. 43–50.
6. Ryabova O. V. Znachenie instituta «elektronnykh dokazatelstv» v otechestvennom ugolovnom sudoproizvod stve // Mirovye issledovaniya v oblasti sotsialno-gumanitarnykh nauk: materialy III Mezhdunarodnoy nauchno-prakticheskoy konferentsii. — Ryazan, 2023. — S. 374–377.
7. Titova K. A., Litvinova I. V. K voprosu o vozmozhnosti primeneniya sushchestvuyushchikh kriteriev dopustimosti dokazatelstv k elektronnym dokazatelstvam v rossiyskom ugolovnom protsesse // Nauchnyy vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Lukyanova. — 2022. — № 2. — S. 144–152.
8. Antwi-Boasiako A., Venter H. A Model for Digital Evidence Admissibility Assessment // 13th IFIP International Conference on Digital Forensics (DigitalForensics), January 2017, Orlando, FL, United States. — Springer, 2017.
9. Goodison S. E., Davis R. C., Jackson B. A. Digital Evidence and the U. S. Criminal Justice System // URL: https://www.rand.org/pubs/research_reports/RR890.html.
10. The Admissibility of Electronic Evidence // URL: https://www.foxmandal.in/the-admissibility-of-electronic-evidence/.