УДК 343.1 DOI: 10.17223/23088451/17/9

**О.В. Желева**

# К ВОПРОСУ О ПОНЯТИИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ И КРИТЕРИЯХ ДОПУСТИМОСТИ ИХ ИСПОЛЬЗОВАНИЯ

Рассматривается вопрос применения информационных технологий в процессе доказывания по уголовному делу. На основе анализа отечественной и зарубежной литературы приводятся различные позиции относительно понятия «электронное доказательство», примеры использования цифровой информации в качестве доказательств. Делается вывод о критериях допустимости электронных доказательств, предложены законодательные изменения, регулирующие особенности их собирания в уголовном процессе.

**Ключевые слова:** *уголовное судопроизводство, информационные технологии, электронные доказательства, критерии допустимости доказательств, собирание доказательств*

Всеобщая глобализация и информатизация оказали существенное влияние на социальное, экономическое и правовое пространство, что привело к внедрению информационных технологий в традиционные отрасли и сферы деятельности.

В соответствии со ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации» под информационными технологиями понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Использование результатов информатизации наблюдается и в уголовном судопроизводстве: применение технических средств и способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств (ст. 164 УПК РФ), электронных носителей информации в качестве доказательств по уголовным делам о преступлениях экономической направленности (ст. 164.1 УПК РФ), видео-конференц-связи при допросе свидетелей в ходе судебного разбирательства (ст. 278.1 УПК РФ) и другие. При этом развитие цифровых технологий в уголовном судопроизводстве продолжается, в литературе указываются следующие его направления: создание информационного учения о доказательствах; переход на электронный документооборот, в том числе электронное уголовное дело; модернизация следственных и судебных действий; использование математических методов, алгоритмов при принятии процессуальных решений; внедрение в уголовный процесс робототехники [1. С. 620].

Признавая влияние информационных технологий на уголовно-процессуальную деятельность, ученые-процессуалисты разрабатывают новые концепции теории доказывания и вводят в употребление новую терминологию «электронное доказательство» [2. С. 3586–3590], «цифровое доказательство» [3. С. 130–134], «цифровая информация» [4. С. 108–110], «электронный носитель информации» [5. С. 44–45], определения которых не содержатся в уголовно-процессуальном законодательстве. Наряду с этим не представляется убедительной позиция о том, что «вопрос определения электронного доказательства», закрепленного на электронном носителе, должен решаться в каждом конкретном случае с соблюдением норм уголовно-процессуального законодательства [6. С. 122]. Такой подход не позволяет определить место электронных доказательств среди иных видов, их отличительные черты, которые обусловливают особенности собирания, использования в уголовном судопроизводстве. В целом в научной литературе отсутствует единое представление о понятии и сущности электронного доказательства. Как следствие в юридической доктрине можно выделить следующие позиции.

Согласно первой электронные доказательства представляют собой вещественные доказательства, которые имеют невербальную форму, могут служить средством к обнаружению преступления, установлению фактических обстоятельств дела, выявлению виновных либо к опровержению обвинения или смягчению ответственности [7. С. 257]. По мнению В.Б. Вехова, сведения, имеющие электронную форму, должны признаваться доказательствами только если они: использовались в качестве орудия преступления; имеют на себе следы преступления; являются предметом преступления или имуществом, полученным в результате преступных действий или средством для обнаружения преступления, способствуют установлению обстоятельств, входящих в предмет доказывания по уголовному делу [8. С. 22].

Сторонники второй позиции утверждают, что электронное доказательство относится к категории иных документов в случаях, если оно содержит соответствующие реквизиты (электронная подпись), лица, интересы которых затрагивает эта информация, не оспаривают ее содержание, а в материалах дела не имеется данных, дающих основание полагать, что указанная информация могла быть сфальсифицирована [9. С. 440]. Представляется, что в данном определении не учитывается, что электронная информация представляет собой не только текстовую информацию (когда компьютер используется в качестве средства фиксации), но и данные, создаваемые автоматически без участия человека, или данные, передаваемые по каналам телекоммуникационных сетей. При этом в число электронных доказательств включается широкий круг информационных источников, к числу которых относят файл, се-

тевой адрес, доменное имя, электронное сообщение, электронный документ, информационную систему, сайт в сети Интернет, страницу сайта в сети Интернет, электронную подпись, программу для электронных вычислительных машин, базу данных, электронный журнал, электронные денежные средства [10. С. 14–15].

Третья позиция заключается в понимании электронных доказательств в качестве информации в электронно-цифровом формате, происходящей от человека, объекта или процесса, зафиксированной на любом материальном носителе, доступной для восприятия и интерпретации (понимания) участниками судопроизводства, происхождение которой не сопряжено с нарушениями закона, представленной в суд в установленном законом порядке и способной обеспечить правильное разрешение уголовного дела по существу [11. С. 72]. Вместе с тем такая информация, по мнению П.С. Пастухова и В.В. Терехина, может иметь три разновидности: иной документ, вещественное доказательство, заключение компьютерно-криминалистической экспертизы [11. С. 73]. Основываясь на определении электронных доказательств как информации, в Будапештской конвенции преступности в сфере компьютерной информации ETS № 185 от 23 ноября 2001 г. предусмотрены такие виды доказательств, как: информация о пользователе, данные трафика, содержательные данные (ст. 1, 18, 20 и 21 Конвенции). А.Ю. Черданцев дополняет этот перечень следующими видами информации: записи транзакций; основные деловые записи; почтовый трафик; записи, хранящиеся у третьих лиц (например, провайдер облачных данных); журналы контроля доступа; конфигурация, события, ошибки и другие внутренние файлы; журналы интернет-активности; антивирусные «логи»; журналы обнаружения вторжений; резервные носители; телефонные журналы; телефонные записи; записи «закрытой системы видеонаблюдения» [12. С. 57–58].

Некоторые авторы конкретизируют содержание третьей позиции, указывая, что электронное (цифровое) доказательство – это не просто информация, а знание, то, что уже включено в процесс доказывания, т.е. отобрано, проинтерпретировано, истолковано согласно когнитивной предуготовленности субъектом доказывания, который использует сведения для выстраивания своей позиции, версии, для убеждения суда [13]. Н.А. Иванов утверждает, что цифровая информация приобретает статус полноценного доказательства только в случае обнаружения, задокументирования и преобразования ее в письменно-изобразительную форму, после чего ее содержание будет доступно для восприятия всеми участниками уголовного процесса [14. С. 100]. В то же время другие ученые справедливо отрицают тождественность понятий «электронное доказательство» и «информация», отмечая, что любая информация первична, а доказательство – это всегда результат уголовно-процессуальной проверки и оценки лицом сведений, полученных в ходе производства по уголовному делу [1. С. 621]. Кроме того, определение электронных доказательств в качестве информации, существующей в электронно-цифровом формате, не позволяет установить отличие природы данного вида доказательств от иных, которое выражается не только в форме представления сведений, но и в особом процессе создания и закрепления информации.

Заслуживает внимания и позиция процессуалистов, которые считают некорректным называть доказательства «электронными», обосновывая это тем, что электронная среда (Интернет), электронные средства сохранения и передачи информации являются хранителями информации аналогично электронному микроскопу [15. С. 67]. Между тем с такой позицией сложно согласиться, поскольку электронные доказательства не только воспроизводятся, но порой и создаются с помощью электронных устройств и содержатся в них.

Если обратиться к международным актам и зарубежному законодательству, то определение понятия «электронные доказательства» также неоднозначно. Так, в соответствии с Концепцией электронных доказательств, предложенной Национальным институтом информационных технологий-INTECO Испании, электронное доказательство представляет собой данные, которые хранятся в цифровой форме или которые были переданы через компьютеры и собраны с помощью специализированных технических инструментов, используемых экспертом в области компьютерных исследований [16].

Согласно Закону Индонезии № 11 от 2008 г. «Об информации и электронных сделках» [17] цифровые (электронные) доказательства понимаются как электронная информация или электронный документ. Исходя из положений данного закона электронные доказательства можно разделить на следующие типы: файл, аудиофайл, удаленный файл, видеофайл, потерянный файл, файл изображения, резервный файл, электронная почта, файл журнала, имя пользователя и пароль, зашифрованный файл, SMS, MMS, BBM, файл стенографии, журнал вызовов и служебный файл.

На основе анализа рассмотренных позиций можно прийти к выводу об убедительности позиции тех авторов, которые относят электронное доказательство к новому виду доказательств [18. С. 143]. Действительно, электронное доказательство обладает особой формой представления и средой существования, формируется человеком и (или) машиной, требует специального способа введения в уголовный процесс, способствует установлению наличия или отсутствия обстоятельств, подлежащих доказыванию по данному уголовному делу.

Преимущество электронных доказательств заключается в том, что информация, содержащаяся на электронных носителях, является объективной, лишена влияния субъективных факторов, таких как возрастные, половые, этнические и профессиональные различия восприятия и запоминания, социально-психологические закономерности восприятия человека человеком, психическое состояние индивида и особенности его речевой деятельности. Кроме того, технические средства копирования, хранения и передачи электронной информации могут сделать ненужными бумажные уголовно-процессуальные документы.

В правоприменительной деятельности распространенным стало использование в качестве доказательств

скриншотов сообщений с телефона (Приговор Советского районного суда г. Томска № 1-25/2019 1-377/2018 от 9 декабря 2019 г. по делу № 1-275/2018 [20]), распечаток переписок из социальных сетей (Приговор Советского районного суда г. Томска № 1-192/2018 от 19 июня 2018 г. по делу № 1-192/2018 [21]), удаленных аудиосообщений, которые хранятся в памяти iPhone (Приговор Кировского районного суда г. Томска № 1-14/2019 1-406/2018 от 21 мая 2019 г. по делу № 1-14/2019 [22]), переписок в приложении WhatsApp (Приговор Стрежевского городского суда № 1-26/2018 от 7 июня 2018 г. по делу № 1-26/2018 [23]) и т.д. При этом такая информация представляется в ходе судебного разбирательства не только стороной обвинения, но и стороной защиты.

В зарубежных странах сфера использования электронных (цифровых) доказательств еще шире. Так, в одном из уголовных дел, возбужденному по факту совершения убийства, в качестве доказательства использовались данные, собранные с устройства Echo, принадлежащего подозреваемому. Во время совершения преступления через динамик Echo велась трансляция музыки, однако после произнесения соответствующего слова активировался виртуальный помощник Alexa, который начал вести запись всех фоновых разговоров. Данная запись была одним из ключевых обвинительных доказательств.

В другом деле источником доказательства стал Snapchat. Благодаря данному приложению пользователи снимают и передают любые изображения, к которым имеется доступ лишь ограниченное количество времени. Между тем в компании действует политика сохранения журналов с данными пользователей в течение 31 дня. В связи с этим эксперты в области цифровой криминалистики смогли получить доступ к журналам и воссоздать отправленные через приложение Snapchat удаленные снимки, на которых было запечатлено совершение преступления [19. С. 22–23].

В то же время особенности электронных доказательств как средств доказывания, обусловленные способом и субъектом их хранения (значительная часть данных может храниться специальным субъектом – провайдером), вызывают сложности с собиранием доказательств и дальнейшим их использованием. Цифровые доказательства непрочны и непостоянны. Неограниченный доступ к цифровой информации создает угрозу фальсификации или уничтожения информации без следов, что требует создания новых методов защиты целостности цифровых данных, обеспечивающих достоверность и допустимость полученной таким образом информации, ее безопасности и сохранности, исключающих возможность раскрытия персональных данных, кражи коммерческой, профессиональной, служебной и государственной тайны. Подлинность информации ставится под сомнение при ее многократном обмене между пользователями, приложениями, компьютерными системами, технологическое устаревание требует обновления или замены оборудования и (или) программного обеспечения, которое используется для хранения, обработки и передачи одной и той же информации. Кроме того, некоторые доказательства могут быть утеряны, когда выключена компьютерная система.

Указанные обстоятельства определяют критерии допустимости электронных доказательств и особенности их собирания. Представляется, что как и другие виды доказательств, электронные доказательства должны соответствовать критериям достоверности (подтверждать реальные факты), допустимости (иметь форму, отвечающую требованиям закона), относимости (должна существовать логическая связь между доказательствами, сведениями и обстоятельствами преступления).

Говоря о критериях допустимости, отечественные ученые-процессуалисты указывают, что данный вид доказательств должен подлежать идентификации (определение субъекта создания и модификации), аутентификации (определение подлинности), верифицируемости (определение даты, времени и способа создания и модификации), быть целостным (неизменным) и воспроизводимым (способность демонстрации доступным способом) [1. С. 620].

В зарубежной литературе отмечается, что электронное доказательство должно быть приемлемо, достоверно, полно и надежно, проверка на соответствие данным критериям осуществляется в многоэтапном процессе собирания доказательств [24. С. 142]. Первый этап – этап изъятия доказательств, в ходе которого следователь определяет, где находится доказательство, где оно хранится, как оно может быть использовано для целей расследования. В зависимости от предполагаемых фактов и связи предполагаемых доказательств с ними выделяют: реальные доказательства (программное обеспечение, представленное для доказательства факта владения цифровыми или цифровыми изображениями); документальные доказательства (электронные письма); косвенные доказательства (файлы журналов, отметки времени файлов, все виды системной информации, используемой для восстановления последовательности событий); свидетельство (нотариальные цифровые документы с цифровой подписью). Второй этап – тестирование электронных доказательств – состоит из обработки и извлечения соответствующей информации из множества собранных данных. Вместе с тем не допускается использование механизмов сжатия, шифрования и контроля доступа, поскольку даже небольшое изменение цифровых доказательств может отразиться на результатах расследования. Третий этап – этап анализа, который включает в себя идентификацию пользователя или внешнего пользователя, местоположения, устройства, совершаемых действий. При этом осуществлять анализ указанных компонентов необходимо в системе. Четвертый этап – этап отчетности, который представляет собой процесс документирования полученной информации.

Повышенные требования к допустимости применение электронных доказательств в России и зарубежных странах обусловлены, прежде всего, тем, что в уголовном процессе, где наиболее ограничиваются конституционные права граждан, использование цифровых тех-

нологий должно сопровождаться установлением надежных средств минимизации рисков и повышенных гарантий. Как верно указывают Ю.В. Гаврилин и А.В. Победкин, «задача цифровых технологий в уголовном судопроизводстве – не заменить процессуальную форму, не выхолостить традиционные гарантии правильного установления обстоятельств по уголовному делу, а оптимизировать порядок производства, облегчить работу должностных лиц, осуществляющих производство по уголовному делу» [25. С. 31].

Основываясь на положениях о недопустимости сокращения объема процессуальных гарантий при использовании электронных доказательств, необходимости обеспечения получения достоверных сведений в ходе собирания доказательств, создания гарантий информационной безопасности при использовании цифровых ресурсов, можно выделить следующие особенности собирания электронных доказательств.

Во-первых, соблюдение общих принципов собирания доказательств. Во-вторых, участие в собирании доказательств специалиста, имеющего специальные устройства и программное обеспечение. В-третьих, до и во время собирания цифровых доказательств никакие действия не должны вызывать изменение цифровых доказательств. В-четвертых, все действия, связанные с собиранием, хранением, доступом или передачей цифровых доказательств, должны быть задокументированы, сохранены и доступны для проверки лицами, чьи интересы могут быть затронуты производством данного процессуального действия (потерпевший, подозреваемый, обвиняемый, защитник и др.). В-пятых, должностное лицо, работающее с электронными доказательствами, должно нести ответственность за всю деятельность, осуществляемую с ними. В-шестых, обеспечение надлежащей передачи или транспортировки цифровых доказательств, а также соответствующих условий для их хранения в зависимости от категории, содержащейся в ней информации.

Таким образом, можно прийти к выводу, что электронные (цифровые) доказательства представляют собой сведения, хранящиеся или передаваемые в цифровой форме, которые соответствующие субъекты могут использовать для установления обстоятельств, входящих в предмет доказывания или иных обстоятельств, имеющих значение для уголовного дела. Между тем, учитывая природу электронных доказательств, необходимость обеспечить их эффективное использование при одновременном сохранении гарантий участников уголовного судопроизводства, в уголовно-процессуальном законодательстве следует закрепить понятие электронных доказательств, порядок их собирания, а также права и обязанности властных субъектов, привлекаемых ими лиц (специалистов, экспертов) при осуществлении данной процедуры.

## ЛИТЕРАТУРА


1. *Зуев С.В.* О современной концепции развития информационных технологий в уголовном судопроизводстве (РИТВУС) // Пермский юридический альманах. 2019. № 2. С. 618–629.
2. *Калитин С.В.* Доказательства электронные и цифровые // Концепт: научно-методический электронный журнал. 2014. Т. 20. С. 3586–3590. URL: http://e-koncept.ru/2014/54981.htm (дата обращения: 13.03.2019).
3. *Иванов Н.А.* Цифровые доказательства: понятие и классификация // Криминалистика в системе правоприменения : материалы науч.-практ. конф. М., 2008. С. 130–134.
4. *Мещеряков В.А., Трухачев В.В.* Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. 2012. № 2. С. 108–110.
5. *Федюкина А.Ю.* Электронный носитель информации как доказательство по уголовным делам // Отечественная юриспруденция. 2016. № 12 (14). С. 44–45.
6. *Балашова А.А.* К вопросу о понятии «электронное доказательство // Закон и право. 2018. № 6. С. 120–122.
7. *Краснова Л.Б.* Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 254–260.
8. *Вехов В.Б.* Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22–24.
9. *Ткачев А.В.* Вопросы использования электронных носителей компьютерной информации в уголовном процессе в качестве доказательств иных документов // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 436–442.
10. *Вехов В.Б., Смагоринский Б.П., Ковалев С.А.* Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2 (46). С. 10–19.
11. *Пастухов П.С., Терехин В.В.* К вопросу о понятии и сущности электронных доказательств в уголовном процессе // Вестник Коми Республиканской академии государственной службы и управления. Серия: Государство и право. 2014. № 18. С. 69–75.
12. *Черданцев А.Ю.* Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. Т. 15, № 4. С. 55–60.
13. *Александров А.С.* «Похвала» теории формальных доказательств // Правоведение. 2002. № 4. С. 34–47.
14. *Иванов Н.А.* Цифровая информация в уголовном процессе // Библиотека криминалиста. 2013. № 5 (10). С. 93–102.
15. *Баранов А.М.* Электронные доказательства: иллюзия уголовного процесса XXI в. // Уголовная юстиция. 2019. № 13. С. 64–69.
16. *INTECO.* URL: http://www.inteco.es/wikiAction/Security/Observatory/area_juridica_seguridad/Enciclopedia/Articulos_1/evidencia_electronica_es.2003 (Accessed: 13th November 2020).
17. *National* Library of Indonesia, Law of the Republic of Indonesia Number 11, 2008. URL: http://datahukum.pnri.go.id/undang-undang/ 2008 (Accessed: 13th November 2020).
18. *Зигура Н.А.* Компьютерная информация как вид доказательств в уголовном процессе России : дис. … канд. юрид. наук. Челябинск, 2010. 234 с.

19. *Allen J., Hallene A.* Digital Evidence // American journal of family law. 2018. P. 21–24.
20. *Приговор* Советского районного суда г. Томска № 1-25/2019 1-377/2018 от 9 декабря 2019 г. по делу № 1-275/2018 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/hktokOrwZgbO/ (дата обращения: 16.11.2020).
21. *Приговор* Советского районного суда г. Томска № 1-192/2018 от 19 июня 2018 г. по делу № 1-192/2018 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/24RSMcYqaLr9/ (дата обращения: 16.11.2020).
22. *Приговор* Кировского районного суда г. Томска № 1-14/2019 1-406/2018 от 21 мая 2019 г. по делу № 1-14/2019 // Судебные и нормативные акты РФ. https://sudact.ru/regular/doc/iSJzlY65yMYt/ (дата обращения: 16.11.2020).
23. *Приговор* Стрежевского городского суда № 1-26/2018 от 7 июня 2018 г. по делу № 1-26/2018 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/KK2GDSDjPXxB/ (дата обращения: 16.11.2020).
24. *Syambas R., El Farisi N.* Two-Step Injection Method for Collecting Digital Evidence in Digital Forensics Nana // J. ICT Res. Appl. 2014. Vol. 8, № 2. P. 141–156.
25. *Гаврилин Ю.В., Победкин А.В.* Модернизация уголовно-процессуально формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3 (51). С. 27–38.

*Статья принята к публикации 24.05.2021.*

**On the Concept of Electronic Evidence and the Criteria for Their Admissibility**

*Ugolovnaya yustitsiya – Russian Journal of Criminal Law*, 2021, no. 17, pp. 44–49. DOI: 10.17223/23088451/17/9
*Olga V. Zheleva*, Tomsk State University (Tomsk, Russian Federation). E-mail: zheleva.olga@gmail.com
**Keywords:** criminal proceedings, information technology, electronic evidence, criteria for evidence admissibility, collection of evidence

The article discusses the development of digital technologies in criminal proceedings and the process of proving in criminal cases in the era of global digitalization. Among the aspects that make this theme relevant are the dynamic development of information technologies, the conservatism and tradition of the criminal process, and the lack of proper regulation on this issue. The author aims at defining the concept of "electronic evidence", specifying the list criteria for electronic evidence admissibility in Russian and foreign practice, and establishing the specifics of collecting evidence. The research methodology includes general and private methods of cognition: dialectical, formal-logical, comparative-legal, systemic, analysis and synthesis. The article provides an analysis of various perspectives of electronic evidence: electronic evidence is physical evidence; electronic evidence as belonging to other documents; electronic evidence as information in an electronic digital format obtained from a person, object or process and recorded on any material medium. The author adheres to the fourth position, according to which electronic evidence is an independent type of evidence, with its special form, media, mechanism of formation, and method of transformation into evidence. Providing examples of the use of electronic evidence in the Russian and foreign law enforcement practice, the author indicates their advantages and disadvantages and emphasizes that the complex storing, processing and transmitting digital information in an unchanged form determines the criteria for electronic evidence admissibility. Like other types of evidence, electronic one must meet the criteria of reliability, admissibility, and relevance. In addition, digital evidence should be subject to identification, authentication, verifiability, be complete (immutable) and reproducible. In conclusion, the author dwells on the peculiarities of collecting evidence, which should be enshrined in criminal procedural legislation: a) compliance with the general principles of collecting evidence; b) mandatory participation of a specialist; c) no actions causing a change in digital evidence before and during its collection; d) documenting all actions related to the collection, storage, access or transfer of digital evidence; e) responsibility of an official working with electronic evidence for all activities with it; e) ensuring the proper transmission or transportation of digital evidence, as well as appropriate conditions for its storage, depending on the category of information it contains.

***References***

1. Zuev, S.V. (2019) On the modern concept of development of information technology in criminal proceedings (RITVUS). *Permskiy yuridicheskiy al'manakh – Perm Legal Almanac*. 2. pp. 618–629. (In Russian).
2. Kalitin, S.V. (2014) Electronic and digital evidence. *Kontsept*. 20. pp. 3586–3590. [Online] Available from: http://e-koncept.ru/2014/54981.htm (Accessed: 13th March 2019).
3. vanov, N.A. (2008) Tsifrovye dokazatel'stva: ponyatie i klassifikatsiya [Digital evidence: concept and classification]. *Kriminalistika v sisteme pravoprimeneniya* [Criminalistics in the system of law enforcement]. Proc. of the Conference. Moscow. pp. 130–134.
4. Meshcheryakov, V.A. & Trukhachev, V.V. (2012) The evidence formation on the basis of electronic digital information. *Vestnik Voronezhskogo instituta MVD Rossii – The Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2. pp. 108–110. (In Russian).
5. Fedyukina, A.Yu. (2016) Elektronnyy nositel' informatsii kak dokazatel'stvo po ugolovnym delam [Electronic information carrier as evidence in criminal cases]. *Otechestvennaya yurisprudentsiya*. 12(14). pp. 44–45.
6. Balashova, A.A. (2018) K voprosu o ponyatii "elektronnoe dokazatel'stvo" [On the concept of "electronic evidence"]. *Zakon i pravo*. 6. pp. 120–122.
7. Krasnova, L.B. (2013) Electronic media as material evidence. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki – Izvestiya Tula State University. Economic and Legal Sciences*. 4-2. pp. 254–260. (In Russian).
8. Vekhov, V.B. (2013) Work with electronic evidence in criminal procedure legislation changed. *Rossiyskiy sledovatel' – Russian Investigator*. 10. pp. 22–24. (In Russian).
9. Tkachev, A.V. (2016) Voprosy ispol'zovaniya elektronnykh nositeley komp'yuternoy informatsii v ugolovnom protsesse v kachestve dokazatel'stv inykh dokumentov [Using electronic media of computer information in criminal proceedings as evidence of other documents]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki – Izvestiya Tula State University. Economic and Legal Sciences*. 3-2. pp. 436–442.
10. Vekhov, V.B., Smagorinskiy, B.P. & Kovalev, S.A. (2016) Cyber traces in forensic science. *Sudebnaya ekspertiza – Forensic Examination*. 2(46). pp. 10–19. (In Russian).

11. Pastukhov, P.S. & Terekhin, V.V. (2014) K voprosu o ponyatii i sushchnosti elektronnykh dokazatel'stv v ugolovnom protsesse [On the concept and essence of electronic evidence in criminal proceedings]. *Vestnik Komi Respublikanskoy akademii gosudarstvennoy sluzhby i upravleniya. Seriya: gosudarstvo i pravo*. 18. pp. 69–75.
12. Cherdantsev, A.Yu. (2019) Concept of Digital Evidence, Current Status and Its Role in the Evidentiary Process. *Yuridicheskaya nauka i praktika*. 15(4). pp. 55–60. (In Russian). DOI: 10.25205/2542-0410-2019-15-4-55-60
13. Aleksandrov, A.S. (2002) "Pokhvala" teorii formal'nykh dokazatel'stv ["Praise" to the theory of formal evidence]. *Pravovedenie*. 4. pp. 34–47.
14. Ivanov, N.A. (2013) Tsifrovaya informatsiya v ugolovnom protsesse [Digital information in the criminal process]. *Biblioteka kriminalista*. 5(10). pp. 93–102.
15. Baranov, A.M. (2019) Electronic Evidence: Illusion of the Criminal Process of the 21st century. *Ugolovnaya yustitsiya – Russian Journal of Criminal Law*. 13. pp. 64–69. (In Russian). DOI: 10.17223/23088451/13/12
16. INTECO. (n.d.) [Online] Avaliable from: http://www.inteco.es/wikiAction/Security/Observatory/area_juridica_se guridad/ Enciclopedia/Articulos_1/evidencia_electronica_es.2003. [Accessed: 13th November 2020].
17. National Library of Indonesia. (2008) *Law of the Republic of Indonesia Number 11, 2008*. [Online] Available from: http://datahukum.pnri.go.id/undang-undang/ 2008 [Accessed: 13th November 2020].
18. Zigura, N.A. (2010) *Komp'yuternaya informatsiya kak vid dokazatel'stv v ugolovnom protsesse Rossii* [Computer information as a type of evidence in the criminal process of Russia]. Law Cand. Diss. Chelyabinsk.
19. Allen, J. & Hallene, A. (2018) Digital Evidence. *American Journal of Family Law*. pp. 21–24.
20. The Sovietsky District Court of Tomsk. (2018a) *Prigovor Sovetskogo rayonnogo suda g. Tomska № 1-25/2019 1-377/2018 ot 9 dekabrya 2019 g. po delu № 1-275/2018* [Verdict No. 1-25 / 2019 1-377 / 2018 of the Soviet District Court of Tomsk dated December 9, 2019, Case No. 1-275 / 2018]. [Online] Available from: https://sudact.ru/regular/doc/hktokOrwZgbO/ (Accessed: 16th November 2020).
21. The Sovietsky District Court of Tomsk. (2018b) *Prigovor Sovetskogo rayonnogo suda g. Tomska № 1-192/2018 ot 19 iyunya 2018 g. po delu № 1-192/2018* [Verdict No. 1-192 / 2018 of the Soviet District Court of Tomsk of June 19, 2018, Case No. 1-192 / 2018]. [Online] Available from: https://sudact.ru/regular/doc/24RSMcYqaLr9/ (Accessed: 16th November 2020).
22. The Kirovsky District Court of Tomsk. (2019) *Prigovor Kirovskogo rayonnogo suda g. Tomska № 1-14/2019 1-406/2018 ot 21 maya 2019 g. po delu № 1-14/2019* [Verdict No. 1-14 / 2019 1-406 / 2018 of the Kirovsky District Court of Tomsk of May 21, 2019, Case No. 1-14 / 2019]. [Online] Available from: https://sudact.ru/regular/doc/iSJzlY65yMYt/ (Accessed: 16th November 2020).
23. The Strezhevoy City Court. (2018) *Prigovor Strezhevskogo gorodskogo suda № 1-26/2018 ot 7 iyunya 2018 g. po delu № 1-26/2018* [Verdict No. 1-26 / 2018 of the Strezhevoy City Court dated June 7, 2018, Case No. 1-26 / 2018]. [Online] Available from: https://sudact.ru/regular/doc/KK2GDSDjPXxB/ (Accessed: 16th November 2020).
24. Syambas, N.R. & Farisi, N.El. (2014) Two-Step Injection Method for Collecting Digital Evidence in Digital Forensics. *Journal of ICT Research and Applications*. 8(2). pp. 141–156. DOI: 10.5614/ITBJ.ICT.RES.APPL.2014.8.2.5
25. Gavrilin, Yu.V. & Pobedkin, A.V. (2019) Modernization of criminal procedure in the information society. *Trudy Akademii Upravleniya MVD Rossii – Proceedings of Management Academy of the Ministry of the Interior of Russia.* 3(51). pp. 27–38. (In Russian).


Received: 24 May 2021.