УДК 343.1 С. 65–71

К ВОПРОСУ О ПРОБЛЕМАХ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ (ЭЛЕКТРОННЫХ) ДАННЫХ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Рудаков Б. В.
Южно-Уральский государственный университет
г. Челябинск, Российская Федерация
E-mail: rudakovbv@susu.ru.

Аннотация. Статья посвящена проблемам использования цифровых данных, хранящихся и циркулирующих в информационных телекоммуникационных системах, в ходе производства следственных действий и их дальнейшего использования в качестве доказательств по уголовным делам. Проводится анализ основных проблем использования цифровых (электронных) данных в доказывании по уголовным делам и пути их преодоления, учитывая особенности широкого спектра цифровой информации в современных условиях, а также рассматриваются проблемы, сопряженные с изъятием цифровой информации из компьютерных хранилищ.

Ключевые слова: цифровые данные, электронные данные, документ, цифровые доказательства, уголовное судопроизводство.

Для цитирования: Рудаков, Б. В. К вопросу о проблемах использования цифровых (электронных) данных в доказывании по уголовным делам / Б. В. Рудаков // Правопорядок: история, теория, практика. — 2021. — № 1 (28). — С. 65–71.

ON THE ISSUE OF THE USE OF DIGITAL (ELECTRONIC) DATA IN EVIDENCE IN CRIMINAL CASES

B. V. Rudakov
South Ural State University
Chelyabinsk, Russian Federation
E-mail: rudakovbv@susu.ru.

Abstract. The article is devoted to the problems of using digital data stored and circulating in information telecommunication systems during investigative actions and their further use as evidence in criminal cases. The analysis of the main problems of the use of digital (electronic) data in evidence in criminal cases and ways to overcome them, taking into account the features of a wide range of digital information in modern conditions, is also considered the problems associated with the removal of digital information from computer storages.

Keywords: digital data, electronic data, document, digital evidence, criminal proceedings.

For citation: Rudakov, B. V. On the Issue of the Use of Digital (Electronic) Data in Evidence in Criminal Cases. *Pravoporyadok: istoriya, teoriya, praktika* [Legal Order: History, Theory, Practice], 2021, no. 1 (28), pp. 65–71. (In Russ.)

Ведение

Компьютерная техника, современные телекоммуникационные технологии и, в целом, информация, представленная в цифровом (электронном) виде стали органичными составляющими современной жизни. Как и прочие достижения научного прогресса, компьютерные технологии, основанные на цифровой информации, используются не только во благо человека, общества и государства, но и для совершения преступлений. Спектр криминальных проявлений, использующих возможности современных компьютерных технологий, так же достаточно широк.

Компьютеры, информационные сетевые технологии и электронная информация в настоящее время являются рутинными элементами повседневной действительности.

Процессы информатизации развиваются в современном мире с чрезвычайной скоростью,

что, наряду с глобализацией, приводит к существенным качественным изменениям практически всех сторон деятельности человека. Бурное развитие информационных технологий привело к образованию нового виртуального информационного пространства. Такой мощный процесс не мог не оказать влияние и на преступную деятельность, как объективную составляющую социума.

Современных преступников в глобальной информатизации привлекает множество ее особенностей, не нашедших пока отражения в законодательстве.

Так, в настоящее время существующее информационное пространство фактически не имеет границ, постольку может находится под юрисдикцией какого-либо одного государства лишь частично [3, с. 55], постольку, поскольку на территории конкретного государства находится оборудование, осуществляющее обработку, накопление и передачу информации. Сама же информация передается практически глобально, быстро и без ограничений. Соответственно, преступники получают возможность осуществлять удаленную и, как правило, достаточно стойко зашифрованную связь между соучастниками, находящимися, порой, в различных государствах, что привело в настоящее время к сильнейшему росту количества и массовости экстремистских движений, трудно контролируемый правоохранительными органами оборот денежных средств, полученных преступным путем, возможность реализации наркотических средств и т. п. [10, с. 199]

Описание исследования

Явление информатизации находит отражение и в деятельности по противодействию преступности. Электронные носители информации были включены в Уголовно-процессуальный закон России как новый вид вещественных доказательств[1]. Как и любое явление, информатизация общества несет в себе две единых противоположности.

С одной стороны, цифровые данные образуют, как правило, электронные следы, которые позволяют судить о совершении человеком различных действий с материальными устройствами в информационном пространстве [9, с. 25]. Практика правоохранительной деятельности свидетельствует о том, что работа с такими следами позволяет эффективно выяснить объективную истину по уголовным делам. К электронным следам можно отнести также видеофиксацию расследуемого (фиксируемого) события (его приготовления, совершения или сокрытия), которую можно получить с различных устройств фиксации видеоизображения (автомобильных видеорегистраторов, камер видеонаблюдения, цифровые фотоснимки и видео-, аудиозапись смартфонов и видео-фотокамер, GPS-навигаторов, информацию, сохраненную в памяти различных электронных устройств (терминалы платежных систем банков, паркоматов электронные валидаторы городского транспорта, коммунальных и иных услуг и др. [1; 8, с. 301].

С другой стороны, работа с классическими вещественными доказательствами преступной деятельности прошла достаточно длительный период совершенствования, нашла достаточно полное отражение в процессуальных нормах права и продолжает гармонично развиваться, используя современные достижения науки и техники.

В отличие от «классических» вещественных доказательств, цифровые данные по своей природе виртуальны, могут быть изменены (уничтожены, созданы), и на настоящем этапе развития наук и технологий зачастую не позволяют с достаточной для доказательственной степени объективности выявить и зафиксировать следы таких воздействий и вызывают достаточно обоснованные сомнения в достоверности полученной цифровой информации.

Объективная реальность такова, что в настоящее время законодатель в сфере совершенствования уголовно-процессуального законодательства практически не успевает за развитием информационных технологий. Своевременное определение проблем и отыскание возможных вариантов их преодоления в данном направлении становится как некогда актуальным [6].

Несмотря на то, что в последнее время наблюдается существенный рост активности законодателя в разработке норм, регулирующих получение, собирание и хранение цифровых доказательств, в рассматриваемом направлении остается множество неразрешенных практических вопросов.

Так, несмотря на то, что в настоящее время цифровая информация может существовать не только в электронном виде, уголовно-процессуальный закон ограничивается только более узким определением «электронный носитель информации» (п. 5 ст. 82 УПК РФ) [2] в контексте особенностей хранения такого вида носителя информации.

---

[1] О внесении изменений в УПК РФ : Федер. закон от 28.07.2012 № 143-ФЗ // Официальный интернет-портал правовой информации. — URL: http://www.pravo.gov.ru (дата обращения: 11.01.2021).

[2] Уголовно-процессуальный кодекс Российской Федерации : Федер. закон от 18 декабря 2001 г. № 174-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_34481/ (дата обращения: 11.01.2021).

Сам по себе электронный носитель информации, не заполненный электронной информацией достаточно редко может являться доказательством как таковым — интерес, как правило, представляет именно хранимая на нем информация. Проблемой может явиться и само значение термина «электронный», поскольку, например, на оптическом диске информация хранится строго говоря не в электронной форме, а при бурном развитии технологий кроме электронной формы могут возникнуть и множество других способов хранения информации, основанные на иных явлениях и процессах, не имеющих отношения к электронной форме существования информации.

Проблема ограничения понятия «электронный» в определенной степени решена в Типовом законе ЮНСИТРАЛ[1] об электронной торговле, одобренного 16 декабря 1996 г. Резолюцией 51/162 на 85-м пленарном заседании Генеральной Ассамблеи ООН, в котором в ст. 2 для обозначения подобного рода информационных источников используется термин «datamessage», который можно перевести как «информационное сообщение» (в оригинале перевода используется не совсем удачный для русской стилистики вариант «сообщение данных») и определяется как «информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными, электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими»[2].

Таким образом, представляется целесообразным в свете современных тенденций развития технологий, вместо понятия «электронная информация» использовать термин «машинная информация», а термин «электронный носитель информации» заменить на «машинный носитель информации» как более универсальный[3].

Процедура получения электронных доказательств с различных устройств обработки, накопления и хранения цифровой (электронной) информации так же может содержать ряд правовых проблем.

Согласно п. 2 части 1 статьи 164 УПК РФ «…Электронные носители информации изымаются в ходе производства следственных действий с участием специалиста».

В настоящее время обращение с простыми электронными носителями информации в виде, например, флеш-накопителей является практически бытовым навыком и, по-видимому, уже доступно такому достаточно образованному человеку как обычный эксперт-криминалист или сам следователь. Загруженность следователей в настоящее время достаточно велика, а привлечение специалиста для работы с простыми электронными носителями информации потребует от организатора следственного действия дополнительных организационных усилий. На современном этапе развития информационного общества оценивать риск утери или изменения данных электронных носителей в простейших типичных следственных ситуациях вполне может сам следователь, и только при необходимости принимать решение о привлечении к следственным действиям соответствующего специалиста, руководствуясь ограничениями ст. 164.1. УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий»[4]. Таким образом, предлагается исключить из п. 2 ч. 1 статьи 164 УПК РФ «…Электронные носители информации изымаются в ходе производства следственных действий с участием специалиста» и в случаях, не требующих наличия глубоких специальных познаний, изъятие электронных носителей информации можно производить в отсутствие специалиста.

Другая проблема работы с цифровыми данными возникает в ситуации, когда носитель информации (например, сервер) находится вне территории, непосредственно доступной следователю для проведения изъятия информации в рамках классических видов необходимых для этого следственных действий (осмотр, обыск, выемка). Возможное решение проблемы — направление поручения в соответствующие территориальные следственные подразделения, как правило потребует значительного времени, что сопрягается с возможной потерей необходимой информации из-за возможного намеренного противодействия либо динамики изменения данных работающих устройств обработки информации.

Решением проблемы получения информации с удаленного источника в перспективе могли бы стать варианты развития и введения

[1] Комиссия ООН по праву международной торговли ЮНСИТРАЛ (англ. United Nations Commission on International Trade Law.

[2] Типовой закон ЮНСИТРАЛ об электронной торговле и Руководство по принятию // United Nations Commission On International Trade Law : [сайт]. URL: https://www.uncitral.org /pdf/russian/texts/electcom/05-89452_Ebook.pdf (дата обращения: 11.01.2021).

[3] Далее в статье для исключения разночтений будет использоваться принятый термин «электронный» вместо «машинный».

[4] Уголовно-процессуальный кодекс Российской Федерации.

в процессуальную практику такого вида следственного действия, как дистанционное получение компьютерной (машинной) информации. Данный подход потребует, безусловно, проработки значительного количества процессуальных деталей, внедрения в процессуальную практику специальных элементов электронного делопроизводства и преодоления инертности осторожного в технических новациях законодателя. К сожалению, к настоящему времени даже попытки внедрения в процессуальную практику дистанционного проведения таких, относительно простых в оценке участниками процесса следственных действий, как допрос, предъявление для опознания и т. п. пока отвергается законодателем [5, с. 108].

В пользу возможности в будущем процессуальной реализации дистанционного получения компьютерной информации следует отметить, что такое действие возможно посредством доступа к интересующей информации с компьютера, оснащенным специальным программным обеспечением, управляемого специалистом. При этом достаточно давно существуют и используются в оперативной практике программно-аппаратные средства, позволяющие объективно фиксировать весь спектр необходимых для доказывания данных в отношении получаемых дистанционно информации. По сути, при получении удаленного доступа к интересующему накопителю информации создается программно-аппаратный комплекс, в котором роль интерфейса выполняет компьютер специалиста, а один из носителей данных находится на удалении, но физически связан с интерфейсом. Насколько принципиальным в процессуальном плане является физическая длина проводника между интерфейсом и накопителем интересующей информации? Следует учесть, что и при обычных следственных действиях рабочая станция, управляющая сервером с массивом жестких дисков, содержащих изымаемые данные, может находиться в разных с ним помещениях и соединятся с ним достаточно сложными и физически достаточно длинными каналами передачи данных. С какой дистанции удаления одного компонента от другого в данном случае станет невозможным проведение классических следственных действий, ставящих целью получение компьютерной информации? Для решения подобной проблемы следует учитывать возможности оперативно-розыскной деятельности, в рамках которой с 2019 года[1] был веден такой вид оперативно-розыскного мероприятия как Получение компьютерной информации. При решении вопросов санкционирования таких мероприятий так же следует учитывать, что в момент доступа к интересующей информации специалист и программно-аппаратный комплекс (т. е. по количеству компонентов большая часть системы) будет локализован в пространстве под юрисдикцией конкретных судебных властей и только носитель информации — на удалении.

Полученные в результате оперативно-розыскного мероприятия результаты в дальнейшем будут предоставляться органам дознания, следователю или в суд в соответствии с процедурой, установленной Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд[2].

Возможности развития процессуальных действий с целью дистанционного получения компьютерной информации открывает Конвенция о преступности в сфере компьютерной информации ETS № 185, в соответствии с которой «в случае, когда компетентные органы производят обыск или получают аналогичный доступ к определенной компьютерной системе или ее части… и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части…, и когда такие данные на законном основании могут быть получены из первой системы или с ее помощью, такие органы имели возможность оперативно распространить производимый обыск или иной аналогичный доступ на другую систему» (ст. 19)[3]. Присоединение России к этой конвенции и внесение соответствующих изменений в УПК позволило бы значительно оперативней противодействовать киберпреступности, особенно учитывая, что значительное количество интересующих правоохранительных органы данных хранится на серверах, расположенных за рубежом,

[1] Об оперативно-розыскной деятельности : Федер. закон от 12.08.1995 № 144-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 11.01.2021).

[2] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сентября 2013 г. № 776/703/509/5 07/1820/42/535/398/68 // СПС «Гарант». URL: https://base.garant.ru/70531824/ (дата обращения: 11.01.2021).

[3] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ cons/cgi/ online. cgi?req=doc&base= INT&n=13526#0758338112987414 (дата обращения 11.01.2021).

а так же в физически распределенных облачных хранилищах на которых проведение классических следственных действий либо крайне затруднено, либо в рамках существующих правовых норм и состояния международных взаимоотношений невозможно[1].

В связи с актуальностью рассматриваемой проблемы предлагались возможные пути ее решения посредством внедрения в уголовный процесс такого следственного действия как «обыск посредством удаленного доступа» [4, с. 87].

В качестве одного из аргументов против внедрения в практику «обыска посредством удаленного доступа» приводится то, что в отличие от классического обыска не происходит изъятия самого исходного материального носителя информации, а только лишь копирование информации с него, что, по мнению оппонентов, неминуемо приводит к модификации исходных данных, и, как следствие, утрате ими доказательственного значения. Но ведь и в ходе ставшей классической фиксации обстановки в ходе проведения следственных действий на фотопленку с последующей печатью с нее фотографий на основе фотохимического процесса так же происходит определенная модификация и потеря информации (изменение параметров контрастности, цветности, потеря определенных деталей в следствии ограничения разрешающей способности и т. п.). Тем не менее не предлагается представлять суду саму обстановку на месте следственного действия, а ограничиваются фотографиями. Таким образом, основной проблемой внедрения в практику «обыска посредством удаленного доступа» являются сомнения в полноте достоверности получаемой в результате его проведения информации. В этой связи предлагается для проведения «обыска посредством удаленного доступа» разработать и применять специально разработанное, прошедшее государственную сертификацию программно-аппаратное обеспечение, методику действий и подготовленного и сертифицированного специалиста, которые сведут к допустимому минимуму искажение получаемой информации.

Проблема укрепления степени достоверности представляемой в уголовном процессе информации может быть в значительной степени решена техническими способами.

Современное состояние развития информационных технологий дает возможность аутентификации электронной (цифровой) информации с помощью электронной цифровой подписи[2], которая в соответствии с действующим законодательством обладает юридической силой[3].

Электронная цифровая подпись — это реквизит электронного документа, полученный в результате криптографического преобразования информации (ее шифрования с использованием специального программно- аппаратного обеспечения), позволяющий проверить отсутствие изменения информации (целостности), в электронном документе после формирования электронной подписи под электронным документом, принадлежность подписи владельцу (авторство), а в случае успешной идентификации подписи подтвердить сам факт подписания электронного документа (неотказуемость). Таким образом, сформированная электронная цифровая подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования, а документ изменен после его подписания.

Встраивание в специальные технические средства специализированных программно-аппаратных компонентов с уникальными неизменяемыми электронными цифровыми подписями, привязанными к конкретному устройству, и, соответственно, к формируемой в результате его применения цифровой (электронной) информации наряду с использованием персональной электронной цифровой подписи лицом, проводящим следственное действие, при соответствующем организационном и нормативном обеспечении может в значительной степени решить проблему обеспечения достоверности и допустимости фиксируемой цифровой (электронной) информации [7, с. 50], которую в последующем предполагается использовать в доказывании по уголовным делам.

За рубежом уже достаточно давно внедряются и апробируются методы работы с электронными (цифровыми) материалами

[1] Карташов И. И. «Цифровые доказательства» в уголовном процессе // Центральный научный вестник. 2016. Т. 1, № 15S. С. 23–25. URL: http://cscb.su/n/0115s01/0115s01008.htm (дата обращения 11.01.2021).

[2] Информационная технология Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: ГОСТ Р 34.10-2012 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/gost-r-34-10-2012 (дата обращения 11.01.2021).

[3] Об электронной подписи : Федеральный закон от 06.04.2011 № 63-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru /document/cons_doc_LAW_112701/ (дата обращения: 11.01.2021).

в качестве доказательств [2; 11, с. 137][1, 2, 3], даже в таких далеких странах, как Занзибар[4].

Заключение

Следует признать, что современные процессы информатизации общества однозначно ведут к практически полному отказу в ближайшем будущем от делопроизводства на бумажных носителях как следствие реализации национальной программы «Цифровая экономика Российской Федерации»[5]. Очевидно, что в весьма недалеком будущем процессуальное делопроизводство столкнется с проблемой необходимости отказа от документов на бумажных носителях и перехода к фиксации доказательственной информации в форме электронных (цифровых) документов, включая аудио-, фото-, видеоматериалы в цифровом формате.

[1] Bazin, Philippe. (2008). An Outline of the French Law on Digital Evidence. *Digital Evidence and Electronic Signature Law Review*, Vol. 5, pp. 179–182. URL: http://sas-space.sas.ac.uk/5543/1/1864-2592-1-SM.pdf (дата обращения: 11.01.2021).

[2] Jolita Kančauskienė. Computer forensics and electronic evidence in criminal legal proceedings: Lithuania's experience. *Digital Evidence and Electronic Signature Law Review*, 2019, Vol. 16, pp. 11–24. URL: https://journals.sas.ac.uk/ deeslr/article/ view/5015/4932 (дата обращения: 11.01.2021).

[3] Киберпреступность. Модуль 4 введение в цифровую криминалистику // United Nations Educational, Scientific and Cultural Organization (UNESCO), United Nations Office on Drugs and Crime (UNODC) : [сайт]. URL: https://www.unodc.org/documents/e4j/Cybercrime_Module_4_Introduction_to_Digital_Forensics_RU.pdf (дата обращения: 11.01.2021).

[4] Makulilo, A. B. The admissibility and authentication of digital evidence in Zanzibar under the new Evidence Act. *Digital Evidence and Electronic Signature Law Review*, 2018, Vol. 15, pp. 48–59. URL: journals.sas.ac.uk/deeslr/article/view/4895/4843 (дата обращения: 11.01.2021).

[5] Национальная программа «Цифровая экономика Российской Федерации» // Правительство Российской Федерации : [сайт]. URL: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf (дата обращения 16.01.2020).

Список литературы

1. Зуев, С. В. Цифровое видеопротоколирование в расследовании преступлений: проблемы и перспективы / С. В. Зуев // Технологии XXI века в юриспруденции : материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 г.) / под редакцией Д. В. Бахтеева. — Екатеринбург : УрГЮУ, 2020. — С. 461–464.
2. Информационные технологии в уголовном процессе зарубежных стран : монография / Д. В.Балашов [и др.] ; под ред. С. В. Зуева. — Москва : Юрлитинформ, 2020. — 216 с.
3. Искевич, И. С. Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект / И. С. Искевич, М. Н. Кочеткова, А. М. Попов // Проблемы правоохранительной деятельности. — 2016.— № 4.— С. 54–58.
4. Ищенко, Е. П. О криминалистике и не только : избранные труды / Е. П. Ищенко. — Москва : Проспект, 2016 — 528 с.
5. Овчинникова, О. В. Дистанционные следственные действия: современное состояние и перспективы / О. В. Овчинникова // Юридическая наука и правоохранительная практика. — 2019. — № 1 (47). — С. 108–116.
6. Основы теории электронных доказательств : коллективная монография / А. Н. Балашов [и др.] ; под ред. С. В. Зуева. — Москва : Юрлитинформ, 2019. — 400 с.
7. Рудаков, Б. В. Проблемы использования материалов видео- и звукозаписи, полученных во внепроцессуальном порядке, для формирования доказательственной базы / Б. В. Рудаков // Вестник Тюменского института повышения квалификации сотрудников МВД России. — 2014. — № 2 (3). –2014.— С. 48–52.
8. Скобелин, С. Ю. Современные возможности «электронных» следов в раскрытии и расследовании преступлений / С. Ю. Скобелин // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : материалы Всероссийской научно-практической конференции (Орел, 29 мая 2015 г.). — Орел : Орловский юрид. ин-т МВД РФ им. В. В. Лукьянова, 2015. — С. 301–305).
9. Смушкин, А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин // Законность. — 2012. — № 8. — С. 23–28.
10. Чернышов, В. Н. Проблемы собирания и использования цифровых доказательств / В. Н. Чернышов, Е. С. Лоскутова // Социально- экономические явления и процессы. — 2017. — Т. 12, № 5. — С. 199–203.
11. Biasiotti, M. A., Mifsud Bonnici, J. P., Cannataci, J., Turchi, F. (eds.). *Handling and Exchanging Electronic Evidence Across Europe*. Springer, 2018, 420 p.

References

1. Zuev, S. V. Tsifrovoe videoprotokolirovanie v rassledovanii prestupleniy: problemy i perspektivy / S. V. Zuev // Tekhnologii XXI veka v yurisprudentsii : materialy Vtoroy mezhdunarodnoy nauchno-prakticheskoy

konferentsii (Yekaterinburg, 22 maya 2020 g.) / pod redaktsiey D. V. Bakhteeva. — Yekaterinburg : UrGYuU, 2020. — S. 461–464.

2. Informatsionnye tekhnologii v ugolovnom protsesse zarubezhnykh stran : monografiya / D. V.Balashov [i dr.] ; pod red. S. V. Zueva. — Moskva : Yurlitinform, 2020. — 216 s.

3. Iskevich, I. S. Aktualnye problemy opredeleniya yurisdiktsii pri rassledovanii prestupleniy v informatsionnom prostranstve: mezhdunarodno-pravovoy aspekt / I. S. Iskevich, M. N. Kochetkova, A. M. Popov // Problemy pravookhranitelnoy deyatelnosti. — 2016.— № 4.— S. 54–58.

4. Ishchenko, Ye. P. O kriminalistike i ne tolko : izbrannye trudy / Ye. P. Ishchenko. — Moskva : Prospekt, 2016 — 528 s.

5. Ovchinnikova, O. V. Distantsionnye sledstvennye deystviya: sovremennoe sostoyanie i perspektivy / O. V. Ovchinnikova // Yuridicheskaya nauka i pravookhranitelnaya praktika. — 2019. — № 1 (47). — S. 108–116.

6. Osnovy teorii elektronnykh dokazatelstv : kollektivnaya monografiya / A. N. Balashov [i dr.] ; pod red. S. V. Zueva. — Moskva : Yurlitinform, 2019. — 400 s.

7. Rudakov, B. V. Problemy ispolzovaniya materialov video- i zvukozapisi, poluchennykh vo vneprotsessualnom poryadke, dlya formirovaniya dokazatelstvennoy bazy / B. V. Rudakov // Vestnik Tyumenskogo instituta povysheniya kvalifikatsii sotrudnikov MVD Rossii. — 2014. — № 2 (3). –2014.— S. 48–52.

8. Skobelin, S. Yu. Covremennye vozmozhnosti «elektronnykh» sledov v raskrytii i rassledovanii prestupleniy / S. Yu. Skobelin // Ugolovno-protsessualnye i kriminalisticheskie problemy borby s prestupnostyu : materialy Vserossiyskoy nauchno-prakticheskoy konferentsii (Orel, 29 maya 2015 g.). — Orel : Orlovskiy yurid. in-t MVD RF im. V. V. Lukyanova, 2015. — S. 301–305).

9. Smushkin, A. B. Virtualnye sledy v kriminalistike / A. B. Smushkin // Zakonnost. — 2012. — № 8. — C. 23–28.

10. Chernyshov, V. N. Problemy sobiraniya i ispolzovaniya tsifrovykh dokazatelstv / V. N. Chernyshov, Ye. S. Loskutova // Sotsialno- ekonomicheskie yavleniya i protsessy. — 2017. — T. 12, № 5. — S. 199–203.

11. Biasiotti, M. A., Mifsud Bonnici, J. P., Cannataci, J., Turchi, F. (eds.). *Handling and Exchanging Electronic Evidence Across Europe*. Springer, 2018, 420 p.

Дата поступления статьи: 14.01.2021.