УДК 343.9

DOI 10.25205/2542-0410-2019-15-4-55-60

Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе

А. Ю. Черданцев

*Московская академия Следственного комитета Российской Федерации
Москва, Россия*

Аннотация

Анализируется международное современное состояние понятия цифровых доказательств, их значение, виды и роль в процессе доказывания по уголовным делам в практической деятельности органов предварительного расследования Российской Федерации. Рассматриваются некоторые проблемы, возникающие в правоприменительной практике, предлагается авторская классификация современных цифровых следов, изучается и сопоставляется международная практика, регламентирующая практическое применение цифровых доказательств, их понятие и содержание. Рассматривается проблема пробелов в правовом регулировании цифровых доказательств, возможность внесения в действующее законодательство изменений, касающихся юридического признания цифровых доказательств наряду с традиционными видами доказательств, а также регламентирования использования цифровых доказательств в уголовном процессе, высказано предложение о внесении ряда изменений в действующее законодательство Российской Федерации, где необходимо закрепить определение цифровых доказательств, тем самым легализовав их, изложив в следующей редакции: цифровые (электронные) доказательства – это информация, хранящаяся или передаваемая в двоичном виде, которая сохранила сведения о подлежащих установлению обстоятельствах уголовного дела в процессе собирания, проверки и оценки доказательства. При этом отмечается, что нет необходимости во введении отдельной статьи для регламентирования цифровых (электронных) доказательств, поскольку определить объем цифровых (электронных) доказательств (цифровой криминалистически значимой информации) достаточно тяжело, хотя бы потому, что единого мнения на данный счет нет и не было, кроме того в связи с динамичным развитием электроники, в том числе и персональной, данная норма быстро теряла свою актуальность и требовала внесения изменений, создавая определенный пробел правового регулирования, что усложняло бы правоприменительную практику.

Ключевые слова

цифровые доказательства, классификация цифровых доказательств, электронные устройства, использование цифровой информации, доказывание, виртуальные следы

Для цитирования

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. DOI 10.25205/2542-0410-2019-15-4-55-60

Concept of Digital Evidence, Current Status and Its Role in the Evidentiary Process

A. Yu. Cherdantsev

*Moscow Academy of the Investigative Committee of Russian Federation
Moscow, Russian Federation*

Annotation

The article analyzes the international current state of the concept of digital evidence, its meaning, types and role in the process of proving in criminal cases in the practical activities of the preliminary investigation bodies of the Russian Federation, considers some problems arising in law enforcement practice, suggests the author's classification of mod-

© А. Ю. Черданцев, 2019

ern digital traces, studies and compares international practice governing the practical application of digital evidence, their concept and content. The problem of gaps in the legal regulation of digital evidence is considered, as well as the possibility of introducing amendments to the current legislation concerning the legal recognition of digital evidence along with traditional types of evidence, as well as the regulation of the use of digital evidence in criminal proceedings, and a proposal is made to introduce a number of amendments to the current legislation of the Russian Federation, where it is necessary to secure definitions of digital evidence, thus legalizing it, stating in the following re At the same time, it is noted that there is no need to introduce a separate article to regulate digital (electronic) evidences, because it is rather difficult to determine the volume of digital (electronic) evidences (digital criminally significant information), at least because there is no unanimity in this respect and there was no unanimity, besides, due to the dynamic development of electronics, including personal ones, this norm quickly lost its relevance and required amendments, creating a certain gap in legal regulation, which is more complicated.

Keywords

digital evidence, classification of digital evidence, electronic devices, use of digital information, evidence, virtual traces

For citation

Cherdantsev A. Yu. Concept of Digital Evidence, Current Status and Its Role in the Evidentiary Process. *Juridical Science and Practice*, 2019, vol. 15, no. 4, p. 55–60. (in Russ.) DOI 10.25205/2542-0410-2019-15-4-55-60

В настоящее время с развитием цифровых технологий, все большей доступностью персональных цифровых устройств и их разнообразием, а также повсеместным распространением сети «Интернет» устранены географические признаки преступности как таковой. Теперь не обязательно находиться в конкретной стране, чтобы совершить преступление на ее территории, для этого достаточно персонального компьютера или даже смартфона с выходом в Интернет. Соответственно и выявлять преступников стало намного сложнее.

В связи с этим в последние несколько лет все большую обеспокоенность вызывает необходимость разработки нормативно-правовой базы, позволяющей в полной мере использовать различные технические средства и аппаратно-программные комплексы для обнаружения, фиксации и изъятия цифровых следов, содержащихся в памяти электронных устройств. В отличие от других форм вещественных доказательств, цифровые доказательства могут создаваться практически мгновенно, буквально за несколько быстрых нажатий клавиш или даже без непосредственного участия человека. Цифровые доказательства предоставляют совокупность уникальных данных, которые зачастую не могут быть доступны в конкретной форме, как в классической криминалистике. Одним из определений цифровых доказательств является интерпретация данных либо инертных (когда они находятся на жестком диске), либо находящихся в движении (сетевые коммуникации), либо их комбинации.

Есть и другие общепринятые определения, которые были даны ведущими организациями и авторами, и служат для описания теории «цифровых доказательств». Так, «Научная рабочая группа по цифровым доказательствам» (Scientific Working Group on Digital Evidence, SWGDE) определяет цифровые доказательства как информацию доказательной ценности, которая хранится или передается в двоичной форме¹; Международная организация сотрудничества в области оценки (International Organization for Cooperation in Evaluation, IOCE) определяет цифровые доказательства как информацию, хранящуюся или передаваемую в двоичной форме, на которую можно сослаться в суде². Оригинальные цифровые доказательства – это физические предметы, содержащие электронные данные, и сами электронные данные, полученные с этих предметов, которые связаны непосредственно с этими предметами или какими-то событиями, получаемые во время изучения. Дубликат цифровых доказательств (Duplicate Digital Evidence) – это точное цифровое воспроизведение всех объектов данных, содержащихся в исходном физическом объекте, копия – это точное воспроизведение

¹ Официальный сайт Scientific Working Group on Digital Evidence. URL: <https://www.swgde.org/> (дата обращения 18.10.2019).

² Официальный сайт International Organization for Cooperation in Evaluation. URL: <https://www.ioce.net/> (дата обращения 18.10.2019).

информации, содержащейся в объектах данных, независимо от исходного физического объекта. Ассоциация руководителей полиции (Association of Chief Police Officers, АСРО) определяет компьютерные электронные доказательства как информацию и данные следственного значения, которые хранятся на компьютере или передаются с помощью компьютера³. Цифровое место преступления – это данные, содержащиеся в цифровом устройстве, таком как жесткий диск или mp3-плеер, найденные на месте физического преступления. Использование термина «цифровые доказательства преступления» признает, что простое присутствие данных на месте физического преступления (в виде хранения на цифровом устройстве) еще не делает их доказательствами.

Наконец, согласно общепринятому международному определению в области криминалистики цифровое доказательство – это любая информация в цифровом виде, которая имеет доказательную силу и может быть использована в качестве достоверного доказательства в суде.

Следовательно, цифровое доказательство – это любая информация, сгенерированная, обработанная, сохраненная или переданная в цифровом виде, которая может быть принята судом в качестве достоверного доказательства, а также другие возможные копии оригинальной цифровой информации, имеющие доказательственную ценность, на которую может ссылаться суд в ходе принятия решения.

Вместе с тем легального определения цифровых доказательств, цифровой криминалистически значимой информации в уголовно-процессуальном законодательстве Российской Федерации, к сожалению, нет. Статьей 74 Уголовно-процессуального кодекса Российской Федерации цифровые доказательства в качестве доказательств не закреплены вовсе, это является одной из наиболее серьезных проблем, определяющих современное состояние цифровых доказательств. Они попросту юридически существуют вне правового поля, что негативно сказывается на целях уголовного процесса. При этом законодатель ограничивается лишь упоминанием понятия «электронные носители информации» при описании особых правил их изъятия в ст. 164.1 УПК РФ, опять же не раскрывая содержания данного понятия в ст. 5 УПК РФ и иных статьях Кодекса, в которых упоминается данное понятие⁴.

Трудно переоценить, насколько обширным является тот объем криминалистически значимой информации, который органы предварительного расследования в настоящее время уже могут получить, обладая специальными познаниями и необходимой техникой. Сложно дать точную и ограничительную классификацию всех потенциальных источников цифровых доказательств по причине того, что электронные средства развиваются стремительными темпами, и вместе с ними растет количество разновидностей и объем цифровых криминалистически значимых данных, но вместе с тем отрицать их значения в уголовном процессе в качестве эффективного и осовремененного вида доказательств просто недальновидно. Можно привести различные примеры источников цифровой информации, выявить их виды и, как следствие, современное состояние из опыта профессиональной деятельности автора настоящей работы.

Так, исходя из практики, полагали бы разумным разделение источников цифровой криминалистически значимой информации по источнику формирования:

- основные записи транзакций – к ним относятся все покупки, продажи и другие договорные соглашения, совершенные в безналичной среде;
- основные деловые записи – к ним относится все вышеперечисленное, а также все документы и данные, которые, вероятно, понадобятся для соблюдения правовых и нормативных требований (договоры, соглашения, отправленные средствами электронной почты и т. д.);

³ Официальный сайт Association of Chief Police Officers. URL: <https://www.npcc.police.uk/> (дата обращения 18.10.2019).

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 27.12.2018, с изм. и доп., вступ. в силу 08.01.2019). URL: www.consultant.ru/cons_doc_LAW_34481 (дата обращения 18.10.2019).

- почтовый трафик – электронные письма потенциально предоставляют важные доказательства официальных и неофициальных контактов;
- записи, хранящиеся у третьих лиц, например, провайдер облачных данных (облачные хранилища данных);
- отдельные индивидуальные персональные компьютеры;
- отдельные мобильные телефоны / смартфоны, планшеты / КПК и носимые устройства и т. д.;
- носители данных – большинство пользователей компьютеров полностью или частично архивируют свои действия на внешних носителях, к ним относятся CD-диски, цифровые универсальные диски (DVD), дискеты, магнитная лента, внешние жесткие диски, карты памяти и флэш-накопители с универсальной последовательной шиной (USB);
- журналы контроля доступа – все цифровые устройства, кроме самых простых компьютерных систем, требуют пароль или аутентифицирующее устройство, прежде чем разрешить вход;
- конфигурация, события, ошибки и другие внутренние файлы и журналы – все компьютеры содержат файлы, которые помогают определить, как должна работать операционная система;
- журналы интернет-активности;
- антивирусные «логи» – с вышеупомянутыми журналами связаны журналы, созданные корпоративными установками антивирусного программного обеспечения, они регистрируют обнаружение и уничтожение вирусов и «троянов», обычная тактика защиты заключается в предположении, что подозрительное поведение было вызвано мошеннической программой, антивирусные журналы часто способствуют разрешению таких сомнений;
- журналы обнаружения вторжений – более крупные компьютерные системы часто используют системы обнаружения вторжений как часть комплексных мер безопасности, они предназначены для обнаружения и предотвращения различных форм взлома;
- резервные носители – все компьютерные системы должны иметь процедуры резервного копирования, чтобы обеспечить быстрое восстановление после возможного полного удаления или программного сбоя;
- телефонные журналы – у операторов связи обычно есть широкие возможности для записи активности пользования абонентским номером;
- телефонные записи – данные предоставлены от текущего контроля, прослушивания и записи переговоров определенных лиц;
- записи «закрытой системы видеонаблюдения» Closed Circuit Television (CCTV) – записи камер видеонаблюдения.

Цифровая криминалистически значимая информация и сами цифровые доказательства по своей природе являются очень хрупкими, поскольку их без особого труда можно легко изменить, подделать или уничтожить в результате неправильного обращения или первоначального изъятия. В связи с этим сотрудники правоохранительных органов, непосредственно осуществляющие работу с цифровыми следами, должны обладать минимальным набором познаний, которые приведут к пониманию специфики обнаружения, фиксации и изъятия цифровой криминалистически значимой информации. В связи с этим в настоящее время представляет научный и практический интерес стандарт ИСО/МЭК 27037:2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме»⁵, который по большому счету является аутентичным переводом международного стандарта ISO/IEC 27037:2012 Информационные технологии – Методы обеспечения безопасности – Руководящие принципы идентификации, сбора, приобретения и сохранения цифровых дока-

⁵ Стандарт ИСО/МЭК 27037:2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме». URL: <http://docs.cntd.ru/document/1200112857> (дата обращения 18.10.2019).

зательств (Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence)⁶, при изучении которого лица, принимающие решения, могут получить сведения, опираясь на которые, можно определить достоверность цифровых доказательств.

Данный стандарт обеспечивает гармонизированную и общепринятую методологию, а также понятийный аппарат для обеспечения ее целостности и подлинности, кроме того, он направлен на содействие обмену цифровыми доказательствами между юрисдикциями различных государств, путем обеспечения согласованности требований и процедур. При рассмотрении этого вопроса следует учитывать и тот факт, что в настоящее время практически все российские суды в своей правоприменительной деятельности так или иначе связаны с исследованием цифровых доказательств. Решения судов частично, а иногда и полностью основаны на них, при этом сложно отрицать тот факт, что процедура исследования данного вида доказательств далека от идеала и имеет ряд существенных недостатков. Правильная демонстрация цифровых доказательств в суде в ходе судебного следствия в настоящее время в Российской Федерации является достаточно абстрактным процессом, в первую очередь из-за того, что национальное законодательство просто не регулирует данный процесс, кроме того, как было описано выше, отсутствует и сильная правовая база, которая будет определять процедуру сбора и хранения цифровых доказательств, а также последующего их использования, в том числе и при необходимости проведения судебной экспертизы в целях анализа цифровых доказательств.

Таким образом, делая вывод, полагается конструктивным рассмотреть предложение о внесении ряда изменений в действующее законодательство Российской Федерации, в частности в положения ст. 5 Уголовно-процессуального кодекса Российской Федерации, где необходимо закрепить определения цифровых доказательств, тем самым легализовав их, изложив в следующей редакции: *цифровые (электронные) доказательства – это информация, хранимая или передаваемая в двоичном виде, которая сохранила сведения о подлежащих установлению обстоятельствах уголовного дела в процессе собирания, проверки и оценки доказательства*; дополнить ст. 74 п. 4.1. «*цифровые (электронные) доказательства*».

При этом следует отметить, что, по нашему мнению, нецелесообразно введение отдельной статьи, по аналогии со ст. 81 Уголовно-процессуального кодекса Российской Федерации для цифровых (электронных) доказательств, поскольку определить объем цифровых (электронных) доказательств (цифровой криминалистически значимой информации) достаточно тяжело, хотя бы потому, что единого мнения на данный счет нет и не было, кроме того в связи с динамичным развитием электроники, в том числе и персональной, данная норма быстро теряла свою актуальность и требовала внесения изменений, создавая определенный пробел правового регулирования, что усложняло бы правоприменительную практику.

Кроме того, с учетом практической деятельности и опыта криминалистических подразделений различных правоохранительных ведомств в действующем уголовно-процессуальном законодательстве должны быть закреплены общие правила для обеспечения эффективного способа сохранения цифровых доказательств, конкретные же способы работы должны регламентироваться ведомственными и межведомственными приказами и методическими указаниями, так как это не находится в области уголовно-процессуального регулирования.

В настоящее же время цифровым доказательствам по аналогии (условной) применяются общие правила сохранения доказательств. Это хоть и кажется разумным, но не учитывает специфику природы цифровой криминалистически значимой информации и цифровых доказательств. Фактически в настоящее время не существует одного компетентного органа, который бы занимался обнаружением, фиксацией, проверкой, анализом и представлением доказательств в цифровой форме. Этим занимаются различные правоохранительные органы,

⁶ Международный стандарт ISO/IEC 27037:2012 «Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence». URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:en> (дата обращения 18.10.2019).

(криминалистические подразделения Следственного комитета России, Министерства внутренних дел, Федеральной службы безопасности и ряд других), но ни в Уголовно-процессуальном кодексе, ни в каких-либо других правовых источниках не содержатся положения об обработке цифровых доказательств данными органами.

В отсутствие актуального и компетентного национального законодательства мы можем только предполагать, каким образом нам следует вести повседневную деятельность с изъятыми цифровыми доказательствами после их сбора.

*Материал поступил в редколлегию
Received
16.12.2019*

Сведения об авторах / Information about the Authors

Черданцев Антон Юрьевич, аспирант кафедры криминалистики Московской академии Следственного комитета Российской Федерации; следователь по особо важным делам Кемеровского следственного отдела на транспорте Западно-Сибирского следственного управления на транспорте Следственного комитета Российской Федерации; старший лейтенант юстиции (ул. Врубеля, 12, Москва, Российская Федерация)

Anton Yu. Cherdantsev, postgraduate student of Criminalistics Section in Moscow academy of the Investigative Committee of Russian Federation; special case investigator of Kemerovo investigative subdivision of West Siberian investigative Department of Transport Investigative Committee of Russian Federation; senior lieutenant of justice (12 Vrubel Str., Moscow, Russian Federation)

cherdantsev@92.sledcom.ru