

ПО ИТОГАМ ВСЕРОССИЙСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ»

УДК 343.13

№ 4 (1) / 2016, с. 46-50

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

Виталий Борисович Вехов

доктор юридических наук, профессор,

член-корреспондент РАН, Заслуженный деятель науки и образования,

Московский государственный технический университет имени Н.Э. Баумана

(национальный исследовательский университет), г. Москва, Российская Федерация

E-mail: v-vehov@mail.ru

С позиций изменившегося уголовно-процессуального законодательства Российской Федерации в статье исследуются актуальные теоретические и прикладные вопросы, связанные с определением понятия электронных доказательств, построением их классификационной системы и определением ее элементов. Рассматриваются проблемы, возникающие в деятельности органов предварительного расследования при работе с доказательствами названного вида.

Ключевые слова: электронные доказательства, компьютерная информация, электронные документы.

ELECTRONIC EVIDENCE: PROBLEMS OF THEORY AND PRACTICE

Vitaly Vekhov

Doctor of Law, Professor,

Corresponding Member of RANH, Honored Worker of Science and Education,
Moscow State Technical University named after N.E. Bauman (national research university),

Moscow, Russian Federation

E-mail: v-vehov@mail.ru

Current theoretical and applied issues related to the definition of «electronic evidence», building its classification system and defining its elements are examined in the article from a position of changed criminal and procedural legislation of the Russian Federation. The problems arising in the activities of preliminary investigation bodies while dealing with called evidence are discussed.

Keywords: electronic evidence, computer information, electronic documents.

Известно, что доказательствами по делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в определенном процессуальным законода-

тельством порядке устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по делу, а также иных обстоятельств, имеющих зна-

чение для правильного рассмотрения и разрешения дела (ч. 1 ст. 74 УПК РФ, ч. 1 ст. 59 КАС РФ, ч. 1 ст. 55 ГПК РФ, ч. 1 ст. 64 АПК РФ)¹. Данные сведения могут быть зафиксированы на любом материальном носителе как человеком (являться продуктом (отражением) мысленной деятельности конкретного лица), так и автоматом (без участия человека по установленному алгоритму), т. е. быть результатом (отражением) работы программы для электронных вычислительных машин (далее – ЭВМ). В обоих указанных случаях рассматриваемые сведения могут быть представлены в электронном виде – в форме компьютерной информации. В соответствии с примечанием 1 к ст. 272 УК РФ она определена как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Синтезируя изложенные юридические определения, представляется возможным сформулировать родовое понятие рассматриваемой дефиниции. Электронные доказательства – это любые сведения (сообщения, данные), представленные в электронной форме, на основе которых суд, прокурор, следователь, дознаватель в определенном процессуальном законодательством порядке устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по делу, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела.

Продолжая исследование выделенной проблематики, отметим, что в последнее время компьютерная информация все чаще становится предметом и средством совершения различных правонарушений, выступает в качестве доказательств в уголовном, административном, гражданском и арбитражном процессах. Например, лица, участвующие в деле, вправе представлять в суд документы, полученные с использованием информационно-телекоммуникационной сети Интернет, а также в электронном виде, в том числе

¹ Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 19 декабря 2016 г.) // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921; Кодекс административного судопроизводства Российской Федерации : федер. закон от 08 марта 2015 г. № 21-ФЗ (ред. от 03 июля 2016 г.) // Собрание законодательства РФ. – 2015. – № 10. – Ст. 1391; Гражданский процессуальный кодекс Российской Федерации : федер. закон от 14 ноября 2002 г. № 138-ФЗ (ред. от 19 декабря 2016 г.) // Собрание законодательства РФ. – 2002. – № 46. – Ст. 4532; Арбитражный процессуальный кодекс Российской Федерации : федер. закон от 24 июля 2002 г. № 95-ФЗ (ред. от 19 декабря 2016 г.) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3012.

в форме электронного документа, подписанныго электронной подписью (п. 2 и 4 ст. 45 КАС РФ, п. 1.1. и 1.2. ст. 35 ГПК РФ, п. 1 ст. 41 АПК РФ). Такие документы выполняются в форме, установленной для этих документов законодательством Российской Федерации, или в свободной форме, если она для них не установлена.

При соблюдении требований, определенных п. 1 ст. 70 КАС РФ, п. 1 ст. 71 ГПК РФ и п. 3 ст. 75 АПК РФ, электронные документы признаются письменными доказательствами. Причем в административном и гражданском судопроизводстве законодатель разрешает использовать в качестве доказательств аудио- и (или) видеозаписи на электронном носителе. При этом лицо или организация, их представляющие либо заявляющие ходатайство об их истребовании, обязаны указать, когда, кем и в каких условиях осуществлялись записи (п. 1 ст. 76 КАС РФ и ст. 77 ГПК РФ). По этому поводу заметим, что в соответствии с Государственным стандартом Российской Федерации ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения» фотодокументом является изобразительный документ, созданный фотографическим способом, а аудиовизуальным – документ, содержащий изобразительную и звуковую информацию.

В отличие от относительно унифицированных административного, гражданского и арбитражного, отечественное уголовно-процессуальное законодательство более консервативно в вопросах, регламентирующих работу с доказательствами исследуемой категории. Анализ ч. 2 ст. 74 УПК РФ и смежных с ней статей показывает, что компьютерная информация допускается в качестве доказательств в уголовном судопроизводстве лишь как вещественные доказательства (ст. 81 УПК РФ) и иные документы (ст. 84 УПК РФ), а именно, если она:

использовалась в качестве средства совершения преступления;

сохранила на себе следы преступления;

является предметом преступления;

может служить средством для обнаружения преступления и установления обстоятельств уголовного дела;

содержит сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию по уголовному делу [1, с. 23].

Результаты, полученные в ходе изучения действующего отечественного законодательства в сфере информации, информационных технологий, защиты информации и

электронного документооборота, позволили нам предложить следующую классификацию электронных доказательств [2, с. 14-15].

1. Файл – поименованная область электронных записей на материальном носителе, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать.

2. Сетевой адрес – идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему.

3. Доменное имя – обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, которая в ней размещена.

4. Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети. К ним относятся так называемые сообщения «электронной почты», «SMS», «MMS» и др.

5. Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием ЭВМ, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

6. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

7. Сайт в сети Интернет – совокупность программ для ЭВМ и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в этой сети.

8. Страница сайта в сети Интернет – часть сайта в сети Интернет, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта.

9. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с ней и используемая для определения лица, подписавшего информацию. По юридической силе законодатель различает простую и усиленную электронные подписи. Последняя в свою очередь подраз-

деляется на неквалифицированную и квалифицированную. Простая электронная подпись – это коды, пароли или иные средства, например «логин» и соответствующий ему пароль, номер платежной карты и «ПИН-код» к ней, которые подтверждают факт формирования подписи определенным лицом. В качестве «логина» для идентификации лица часто используются абонентский номер мобильного телефона или адрес «электронной почты». Неквалифицированной признается электронная подпись, которая:

1) получена, как мы подробно писали ранее, в результате криптографического преобразования информации с использованием ключа электронной подписи [3];

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

Квалифицированная электронная подпись обладает всеми перечисленными признаками и в дополнении к ним имеет два следующих:

ключ ее проверки указан в квалифицированном сертификате;

для ее создания и проверки используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным Федеральным законом «Об электронной подписи»².

С позиций доказывания большое значение имеют следующие обстоятельства:

1) информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписенному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе;

2) электронной подписью могут быть подписаны несколько связанных между собой электронных документов, объединенных в пакет, и при этом каждый из них считается подписанным данной подписью.

² Об электронной подписи : федер. закон от 06 апреля 2011 г. № 63-ФЗ // Собрание законодательства РФ. – 2011. – № 15. – Ст. 2036.

10. Программа для ЭВМ (компьютерная программа) – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

11. База данных – это представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

12. Электронный журнал – документ или совокупность документов в электронной форме, сформированный (сформированных) банкоматом и (или) электронным терминалом за определенный период времени при совершении операций с использованием данных устройств.

13. Электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом (лицом, представившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.

Поскольку названные доказательства находятся в сложных материальных форматах на электронных носителях информации, на что мы обращали внимание ранее [4, с. 157], работа с ними осуществляется в рамках процессуальных действий, к производству которых, как правило, привлекаются специалисты, обладающие знаниями, умениями и навыками в сфере компьютерной информации и электронного документооборота. В отдельных случаях участие в них специалиста является обязательным. Так, например, электронные носители, содержащие доказательственную информацию, возвращаются их законному владельцу после осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания. Однако в случае невозможности их возврата содержащаяся на них информация копируется по ходатайству законного владельца или ее обладателя – лица, само-

стоятельно создавшего информацию либо получившего на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам³. Копирование происходит с участием ее законного обладателя или владельца изъятых электронных носителей и (или) его представителя и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде. Она копируется на другие электронные носители в условиях, исключающих возможность ее утраты или изменения. При этом копирование информации не производится, если это может воспрепятствовать расследованию преступления (п. 5 ч. 2 ст. 82 УПК РФ). По результатам осуществления этого нового процессуального действия составляется протокол (ч. 2.1. ст. 82 УПК РФ), к которому могут прилагаться электронные носители, содержащие информацию, которая была получена или скопирована с других электронных носителей в ходе производства следственного действия (ч. 8 ст. 166 УПК РФ).

При производстве обыска и выемки электронные доказательства также изымаются только с участием специалиста. По ходатайству их законного обладателя или владельца материального носителя, на котором они находятся, специалистом в присутствии понятых осуществляется их копирование на другие электронные носители. Копирование не допускается, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение электронных доказательств. Об этом в протоколе обыска или выемки делается соответствующая запись (ч. 9.1. ст. 182, ч. 3.1. ст. 183 УПК РФ).

Схожий порядок работы с информацией, находящейся на электронных носителях и имеющей доказательственное значение, имеет место при производстве отдельных оперативно-розыскных мероприятий. Например, в ходе проведения сотрудниками органов внутренних дел такого гласного оперативно-розыскного мероприятия, как обследование помещений, зданий, сооружений, участков местности и транспортных средств, перед изъятием информации названного вида сотрудник полиции обязан предоставить лицу, у которого она изымается, возможность изготовить ее копию. При этом должны быть приняты меры к недопущению уничтожения

³ Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. – 2006. – 29 июля. – Ст. 2, п. 5.

информации, находящейся на изымаемых электронных носителях⁴.

Изложенные новеллы отечественного уголовно-процессуального законодательства обусловили возникновение ряда проблем, имеющих как теоретическое, так и прикладное значение. По нашему мнению, наиболее значимыми являются следующие из них.

1. Отсутствие законодательного определения понятия «электронный носитель информации», что позволяет с позиций формальной юридической логики отнести к этой категории достаточно широкий круг предметов и документов. Например, стиральную или кофемашину, микроволновую печь, телевизор, паспорт гражданина Российской Федерации, электронный полис обязательного медицинского страхования, электронный ключ от домофона или системы зажигания автомобиля и др.

2. Малое число и недостаточная доступность для органов предварительного расследования и судов компетентных специалистов, без которых невозможно в установленном уголовно-процессуальным законом порядке провести отдельные следственные действия, связанные с изъятием электронных носителей и копированием с них компьютерной информации, имеющей доказательственное значение.

3. Отсутствие полноценных научно обоснованных рекомендаций по оптимальному получению, оценке и использованию электронных доказательств. В связи с чем в правоприменительной практике очень часто возникают различные процессуальные ошибки. Например, установление вида, юридической силы, срока действия и возможностей использования электронной подписи для удостоверения документов в тех или иных информационных системах (общего

пользования или корпоративных) очень часто осуществляется путем назначения судебной компьютерно-технической экспертизы, что является неправильным. Эти задачи необходимо решать, базируясь на положениях ст. 2 Федерального закона «Об электронной подписи» следующим образом:

1) путем направления письменного запроса в адрес удостоверяющего центра – юридического лица, индивидуального предпринимателя либо государственного органа или органа местного самоуправления, осуществляющего функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации в этой области (п. 7);

2) путем получения показаний владельца сертификата ключа проверки электронной подписи, т. е. лица, которому в установленном законом порядке выдан сертификат ключа ее проверки – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо его доверенным лицом и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи (п. 4 и 2).

По нашему мнению, одним из вариантов выхода из сложившейся негативной ситуации является систематизация имеющихся знаний по данной проблематике в науках юридического цикла, установление научно-важеских связей между существующими теориями (учениями) и выработка общих точек зрения на один и тот же предмет в целях комплексного решения проблем, связанных с получением, фиксацией и использованием электронных доказательств. Все это можно осуществить в рамках одной гипотезы, именуемой «Теория электронных доказательств».

Примечания

1. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. – 2013. – № 10. – С. 22-24.
2. Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики // Судебная экспертиза. – 2016. – № 2 (46). – С. 10-19.
3. Вехов В. Б. Криминалистически значимые сведения об электронной цифровой подписи // Вестник Волгоградской академии МВД России. – 2008. – № 1. – С. 71-80.
4. Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. – М. : Академия Следственного комитета Российской Федерации, 2016. – № 1. – С. 155-158.

⁴ Об утверждении Инструкции о порядке проведения сотрудниками органов внутренних дел гласного оперативно-розыскного мероприятия обследование помещений, зданий, сооружений, участков местности и транспортных средств : приказ МВД России от 30 марта 2010 г. № 249.