УГОЛОВНЫЙ ПРОЦЕСС

DOI: 10.17803/1994-1471.2021.129.8.118-128

М. И. Воронин*

Особенности оценки электронных (цифровых) доказательств[1]

Аннотация. В современной уголовно-процессуальной правоприменительной практике оценка электронных (цифровых) доказательств осуществляется по общим правилам оценки доказательств, регламентированным уголовно-процессуальным законом. При этом нередко судами не учитываются электронная (цифровая) сущность рассматриваемого вида доказательств, что порой приводит к ошибочной уголовно-правовой квалификации деяния либо к иным неправильным выводам в итоговом процессуальном решении. Научное осмысление нового источника информации в системе нормативно установленных доказательств находится в активной фазе (и еще далеко от завершения), однако анализ теоретических воззрений и правоприменительной, прежде всего судебной, практики позволяет выдвинуть предложения о поэтапном реформировании уголовно-процессуального закона и корректировке правоприменения на основе очевидных и не вызывающих принципиальных возражений особенностей электронных (цифровых) доказательств, касающихся их сущности, специфики собирания, проверки и оценки. В статье акцент сделан на таком элементе доказывания, как оценка доказательств, поскольку в силу того, что он менее формализован, суды довольно часто допускают ошибки при оценке относимости, допустимости и достоверности электронных (цифровых) доказательств.

Ключевые слова: уголовный процесс; доказательство; доказывание; электронное доказательство; относимость доказательств; допустимость доказательств; достоверность доказательств; достаточность электронных доказательств; актуальные проблемы; электронное доказывание.

Для цитирования: *Воронин М. И.* Особенности оценки электронных (цифровых) доказательств // Актуальные проблемы российского права. — 2021. — Т. 16. — № 8. — С. 118–128. — DOI: 10.17803/1994-1471.2021.129.8.118-128.

Characteristics of Electronic (Digital) Evidence Assessment[2]

Mikhail I. Voronin, Attorney at Law, "Yukov & Partners" Law Office
Samarskaya ul., 3, str. 1, Moscow, Russia, 129110
m_voronin@bk.ru

Abstract. In modern criminal procedure law enforcement practice, the assessment of electronic (digital) evidence is carried out according to the general rules for assessing evidence, regulated by the criminal procedure law. At the

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16041.

[2] The reported study was funded by RFBR according to the research project № 18-29-16041.МК.

* *Воронин Михаил Ильич*, адвокат, коллегия адвокатов «Юков и партнеры»
Самарская ул., 3 строение 1, г. Москва, 129110
m_voronin@bk.ru

same time, the courts often do not take into account the electronic (digital) nature of the type of evidence under consideration, which sometimes leads to an erroneous criminal legal qualification of the act or to other incorrect conclusions in the final procedural decision. Scientific comprehension of a new source of information in the system of normatively established evidence is in its active phase (and is still far from completion). However, this analysis of theoretical views and law enforcement, primarily judicial, practice makes it possible to put forward proposals for a phased reform of the criminal procedural law and adjusting law enforcement on the basis of obvious and the features of electronic (digital) evidence, which do not cause fundamental objections, concerning their essence, the specifics of collection, verification and evaluation. The paper focuses on such an element of establishment of evidence as evidence assessment, since, due to the fact that it is less formalized, the courts quite often make mistakes when assessing the relevance, admissibility and reliability of electronic (digital) evidence.
Keywords: criminal procedure; proof; establishment of evidence; electronic evidence; relevance of evidence; admissibility of evidence; reliability of evidence; sufficiency of electronic evidence; actual problems; electronic evidence collection.
Cite as: Voronin MI. Osobennosti otsenki elektronnykh (tsifrovykh) dokazatelstv [Characteristics of Electronic (Digital) Evidence Assessment]. *Aktualnye problemy rossiyskogo prava*. 2021;16(8):118-128. DOI: 10.17803/1994-1471.2021.129.8.118-128. (In Russ., abstract in Eng.).

Оценка доказательств в уголовном процессе производится по правилам, предусмотренным УПК. В соответствии со статьей 88 УПК каждое доказательство подлежит оценке с точки зрения относимости, допустимости, достоверности, а все собранные доказательства в совокупности — достаточности для разрешения уголовного дела.

Оценка доказательств представляет мыслительную деятельность субъектов доказывания (следователя, дознавателя, прокурора, судьи), осуществляемую в логических формах при соблюдении методологии познания[3].

Свои особенности имеет оценка электронных (цифровых) доказательств, обусловленная, прежде всего, их электронной (цифровой) природой. Специфика рассматриваемого вида доказательств, механизм их формирования и функционирования, должны приниматься во внимание при реализации положений статьи 88 УПК, о чем, в частности, свидетельствуют материалы следственной и судебной практики. Ошибочная оценка электронных доказательств может привести, в частности, к неправильным выводам о фактических обстоятельствах уголовного дела и неверной уголовно-правовой квалификации совершенного деяния.

1. *Установление исключительно функциональных возможностей электронных (цифровых) доказательств, без учета наличия (отсутствия) иных доказательств, равно как и неправильное установление функциональных свойств данного вида доказательств, может привести к ошибочным выводам об относимости этих доказательств и, как следствие, об уголовно-правовой квалификации совершенного деяния.*

1.1. Так, гр-н П. был осужден за совершение преступления, предусмотренного п.п. «а», «г» ч. 2 ст. 242 УК РФ. Суды признали доказанным совершенное преступное деяние, поскольку П,, используя принадлежащий ему персональный компьютер, имеющий подключение к сети «Интернет», скопировал видеофайлы с порнографическими изображениями несовершеннолетних, поместил указанные файлы в память своего компьютера, используя установленную в памяти компьютера файлообменную программу «Shareaza 2.7.9.0», позволяющую осуществить доступ к файлообменной сети, достоверно зная о функциональных свойствах данной программы, предназначенной для обмена файлами между пользователями локальной сети «Интернет», а также о возможности предоставления общего доступа неограниченному количеству пользователей указанной сети к информации, содержащейся в памяти его персонального компьютера в папке «загрузка», в которую

[3] Теория доказательств в советском уголовном процессе / отв.ред. Н. В. Жогин. М. : Юрид. лит., 1973. С. 427.

поместил видеофайлы с порнографическими изображениями несовершеннолетних, предоставив неограниченному количеству пользователей локальной сети «Интернет» возможность беспрепятственно скачивать указанные видеофайлы, содержащие материалы с порнографическими изображениями несовершеннолетних.

Верховный Суд РФ отменил судебные акты нижестоящих судов и принял решение о прекращении уголовного дела в отношении П. за отсутствием в деянии состава преступления, указав при этом следующее. То обстоятельство, что П. было известно о сохранении скачанных на компьютер файлов порнографического содержания в программе, позволяющей другим пользователям скачивать данные файлы, само по себе не может свидетельствовать об умысле осужденного на их распространение, поскольку на момент приобретения (скачивания, копирования) им данных файлов они уже были распространены в сети «Интернет» и находились в свободном доступе[4].

Иными словами, ВС согласился с тем, что функциональные свойства электронного доказательства сами по себе не являются достаточным основанием для привлечения к уголовной ответственности и не свидетельствуют о наличии в действиях подсудимого состава преступления. Отрадно, что в рассматриваемом деле ВС применил статьи 49 Конституции РФ и 14 УПК о презумпции невиновности, отметив, что стороной обвинения не опровергнуты доводы подсудимого о том, что он специально не занимался скачиванием файлов с порнографическими изображениями несовершеннолетних с целью их последующего распространения.

1.2. По некоторым уголовным делам о преступлениях, предусмотренных статьей 187 УК РФ «Неправомерный оборот средств платежей», суды первой инстанции не учли особенности составообразующих доказательств, допустив ошибку в оценке их относимости к делу, что повлекло за собой отмену приговоров.

Так, гр-н Н. был осужден, в частности, за то, что предоставил свой паспорт с целью внесения в единый государственный реестр юридических лиц сведений о нем, как о подставном лице, за денежное вознаграждение, а после внесения сведений о нем как о директоре и учредителе юридического лица открыл расчетный счет в банке с системой ДБО (дистанционного банковского обслуживания), после чего сбыл прилагающийся к данному счету электронный носитель информации, посредством которого осуществляется доступ к системе ДБО, позволяющий третьим лицам в последующем осуществлять денежные переводы по расчетному счету от имени юридического лица и, в частности, Н. Данным электронным носителем информации являлся ключ электронной подписи. Суд признал Н. виновным в совершении преступления, предусмотренного ч. 1 ст. 187 УК РФ[5].

Отменяя приговор суда первой инстанции, суд кассационной инстанции указал, в частности, что предметами преступления, предусмотренного статьей 187 УК РФ, наряду с иными, являются электронные средства, электронные носители информации, предназначенные для неправомерного осуществления перевода денежных средств. Согласно статье 2 Федерального закона № 63-ФЗ «Об электронной подписи» ключ электронной подписи — это уникальная последовательность символов, предназначенная для создания электронной подписи, а электронная подпись — это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. И далее кассационный суд пришел к выводу о том, что изготовленный и полученный Н. в установленном порядке ключ электронной подписи не может быть отнесен к электронным средствам, электронным носителям информации, предназначенным для неправомерного осуществления перевода денежных средств, поскольку он представлял из себя лишь совокупность последовательных символов, предна-

[4] Кассационное определение Верховного Суда РФ от 10 июля 2019 г. № 16-УД19-7 // СПС «КонсультантПлюс».

[5] Приговор Аннинского районного суда Воронежской области от 6 июля 2017 г. по делу № 1-71/2017 // СПС «КонсультантПлюс».

значенную для создания электронной подписи, которая без присоединения ее к другой информации значимости не имела[6].

Ошибка в оценке электронного доказательства как предмета преступления была допущена также другим судом первой инстанции, признавшим наличие в действиях И. состава преступления, предусмотренного ч. 2 ст. 187 УК РФ. Суд кассационной инстанции, отменяя судебные акты судов первой и апелляционной инстанций, указал, что предмет преступления, предусмотренного ч. 2 ст. 187 УК РФ, составляют только платежные документы, не являющиеся ценными бумагами, которые могут быть использованы в денежно-кредитном обороте, поэтому суд первой инстанции должен был обсудить вопрос, относится ли кассовый чек на ГСМ к указанным документам, применительно к Положению ЦБР от 03 октября 2002 год № 2-П «О безналичных расчетах в Российской Федерации»[7]. Включая это дело в Обзор судебной практики по уголовным делам, Президиум Нижегородского областного суда сделал важное замечание о необходимости при определении понятия «иной платежный документ», вследствие бланкетности нормы статьи 187 УК РФ, руководствоваться тем смыслом понятия, который придается ему в отрасли гражданского права, то есть в качестве предмета данного преступления выступают такие платежные документы, не являющиеся ценнными бумагами, которые могут быть использованы в денежно-кредитном обороте и позволяющие производить наличные и безналичные расчеты[8].

Соответственно, если гражданско-правовая сущность собранных по делу электронных доказательств не позволяет их отнести к иным платежным документам, с учетом диспозиции статьи 187 УК РФ, следовательно, они не обладают свойством относимости и не могут быть признаны доказательствами по уголовному делу.

1.3. По уголовным делам о преступлениях в сфере компьютерной информации важное значение имеет правильное установление технических свойств и характеристик, используемых для совершения преступлений компьютерных программ и иных электронных (цифровых) доказательств.

Так, приговором суда Т. признан виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», и осужден за совершение создания, распространения и использования компьютерных программ, заведомо предназначенных для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации[9].

Ключевым доказательством, признанным судами обеих инстанций относимым, явилась обнаруженная у подсудимого на оптическом диске программа (файлы), детектируемые программой антивирусом как вредоносные.

В другом деле суд, установив функциональные свойства использованных подсудимым С. компьютерных программ ведущих мировых производителей, пришел к выводу, что эти программы не могут быть признаны вредоносными, поскольку были созданы и предназначены не для заведомо несанкционированного доступа к компьютерной информации, а для ее защиты. Суд апелляционной инстанции, в частности, отметил, что компьютерная программа — объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютерного устройства с целью получения определенного результата, а по смыслу статьи 273 УК РФ, под вредонос-

[6] Постановление Президиума Воронежского областного суда по делу № 44у-65/2017 // СПС «КонсультантПлюс».

[7] Постановление Президиума Нижегородского областного суда от 22 января 2019 г. по делу № 44у-851/2009 // СПС «КонсультантПлюс»

[8] Обзор судебной практики Президиума Нижегородского областного суда за 2-й квартал 2009 г. П. 6 // СПС «КонсультантПлюс».

[9] Апелляционное определение Московского городского суда от 17 августа 2016 г. по делу № 10-12939/2016 // СПС «КонсультантПлюс».

ными программами очевидно понимаются программы, известные как компьютерные вирусы, то есть такие программы, которые специально созданы в целях нарушения нормального функционирования компьютерных программ для достижения преступных результатов, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации[10].

2. *Правовой статус электронного (цифрового) доказательства имеет значение для уголовно-правовой квалификации деяния.*

Согласно разъяснениям Пленума Верховного Суда РФ при решении вопроса об использовании средств массовой информации (далее — СМИ), электронных или информационно-телекоммуникационных сетей, в том числе в сети «Интернет» для публичных призывов к совершению террористической деятельности или публичного оправдания терроризма (часть 2 статьи 205.2 УК РФ), необходимо учитывать положения Закона РФ от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» и Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Если публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма совершены с использованием сетевых изданий (сайтов в сети «Интернет»), имеющих правовой статус СМИ (то есть зарегистрированных в таком качестве), то содеянное следует квалифицировать по части 2 статьи 205.2 УК РФ как совершенное с использованием СМИ. Использование для совершения указанных деяний сайтов в сети «Интернет», не зарегистрированных в установленном законом порядке в качестве СМИ, квалифицируется по части 2 статьи 205.2 УК РФ как деяние, совершенное с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»[11].

3. Оценка допустимости электронных (цифровых) доказательств российскими правоприменителями продиктована в большей степени прагматическими соображениями и основана не столько на проверке соблюдения разрозненных и малочисленных норм уголовно-процессуального закона, посвященных электронным доказательствам, что само по себе является серьезной проблемой, сколько на отсутствии понимания особенностей правовой природы электронных доказательств и возможности иными доказательствами установить обстоятельства, входящие в предмет доказывания.

В литературе широко освещались вопросы о спорных подходах судов к оценке допустимости электронных доказательств, такие как:

— законность осмотра мобильного телефона и изучение в ходе него содержащейся в телефоне переписки без судебного решения;
— допустимость выемки переписки гражданина в социальной сети без судебного решения;
— необязательное участие специалиста при изъятии электронных носителей информации и копировании с них информации при производстве следственных действий;
— о необходимости применения на практике концепции «цепи законных владений» — процессуальное документирование в целях сохранности электронного доказательства на всех этапах уголовного судопроизводства, от момента собирания доказательственной информации до передачи ее носителя от одного лиц к другому вплоть до судебного рассмотрения дела;
— отсутствие реализации на практике правовых позиций ЕСПЧ, высказанных им в связи с процедурными аспектами собирания, проверки и оценки электронных доказательств[12].

[10] Апелляционное постановление от 9 февраля 2017 г. по делу № 10-244/17 // СПС «КонсультантПлюс».

[11] Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности». П. 21, 22.

[12] См., например: *Воронин М. И.* Недопустимая допустимость электронных доказательств. Судебная практика и пробелы в УПК // Уголовный процесс. 2020. № 10. С. 46—55.

Оценка допустимости доказательств предполагает установление соответствия порядка получения доказательств нормам уголовно-процессуального права. Иными словами, допустимость доказательств — это пригодность сведений с точки зрения соблюдения уголовно-процессуальной формы служить средством установления обстоятельств по уголовному делу.

На сегодняшний день производимая субъектами доказывания оценка допустимости электронных (цифровых) доказательств достаточно примитивна и во многом произвольна. Это обусловлено прежде всего отсутствием системного нормативно-правового регулирования отношений, связанных с собиранием, проверкой и оценкой электронных (цифровых) доказательств, равно как и с отсутствием в законе определения понятия «электронное (цифровое) доказательство».

Представляется, что решению данной проблемы должны способствовать научные разработки, посвященные электронным доказательствам, основанные, в том числе, на анализе правоприменительной практики и зарубежного опыта.

Правовые новации в этой области вряд ли будут кардинальными, поскольку накапливаемый с годами опыт работы с электронными доказательствами чуть ли не ежедневно ставит перед наукой и практикой все новые вопросы, решение которых по определению не может быть простым и одномоментным. Поэтому, думается, реформирование уголовно-процессуального законодательства в части допустимости электронных доказательств должно происходить в несколько этапов. На первом этапе необходимо выделить в законе в качестве самостоятельного вида доказательства «электронное (цифровое) доказательство», внеся это доказательство в перечень доказательств, закрепленный в части 2 статьи 74 УПК. Вместе с этим, само понятие электронного (цифрового) доказательства нужно включить в статью 5 и в ней же раскрыть это понятие. В рамках этого же этапа дополнить или изменить уже существующие нормы уголовно-процессуального закона, посвященные электронным носителям информации и иным электронным источникам доказывания, положениями, более-менее устоявшимися в теоретических изысканиях и практически реализуемых, включая инкорпорирование в национальное законодательство правовых позиций ЕСПЧ.

На втором этапе целесообразно было бы включить в УПК главу 27.1, в которой закрепить новые виды следственных действий, направленных на собирание электронных (цифровых) доказательств. К таковым могут быть отнесены:

— осмотр сетевых информационных ресурсов[13];
— удаленное подключение к компьютеру в процессе его работы[14];
— выемка электронных носителей информации[15];
— копирование электронной информации[16];
— арест электронно-почтовой корреспонденции[17].

В рамках третьего этапа, с учетом последующих научных разработок, международно-правового опыта и выявленных проблем правоприменения провести систематизацию уголовно-процессуальных норм об электронных (цифровых) доказательствах в рамках глав 10 и 11, дополнив

[13] *Першин А. Н.* Осмотр сетевых информационных ресурсов — новый вид следственного действия? // Российский следователь. 2020. № 1. С. 13—16.

[14] *Бахтеев Д. В., Смахтин Е. В.* Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. УрГЮУ. 2019. № 6. С. 61—68.

[15] *Добровлянина О. В.* Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации // Пермский юридический альманах. 2019. № 2. С. 641—649.

[16] Основы теории электронных доказательств : монография / под ред. С. В. Зуева. М. : Юрлитинформ, 2019. С. 311.

[17] *Овсянников Д. В.* Электронное копирование информации в системе средств уголовно-процессуального доказывания // Правопорядок: история, теория, практика. 2014. № 2 (3). С. 131—132.

их соответствующими статьями об электронных (цифровых) доказательствах и доказывании посредством этого вида доказательств.

Важной составляющей института допустимости электронных (цифровых) доказательств должно стать соблюдение и обеспечение «процессуальной цепи доказательств» — последовательного установления процесса обнаружения, изъятия, закрепления, приобщения и хранения электронных (цифровых) доказательств. Выпадение одного из звеньев этой цепи безусловно должно влечь признание электронного (цифрового) доказательства недопустимым. Теоретической основой такой позиции является доктрина «цепи законных владений», суть которой заключается в сохранении доказательств на всех этапах: от момента сбора доказательственной информации до передачи ее носителя от одного лица к другому вплоть до судебного рассмотрения. Раскрывая эту концепцию в своих публикациях Галяшина Е. И. справедливо замечает, что суд (следователь) должен иметь точную информацию, кто и из какого источника получил доказательство, как оно хранилось, кто имел к нему доступ[18].

Вопрос о допустимости электронных доказательств в практике возникает в тех случаях, когда данные доказательства изымаются без участия специалиста, как того требует ч. 2 ст. 164.1 УПК РФ. Суды, как правило, не видят в этом нарушения норм УПК РФ, поскольку, по их мнению, участие специалиста требуется только в случаях копирования или изучения информации на электронных носителях в месте, где их обнаружили. В том же случае, когда компьютер, телефон и т.д. изымаются целиком необходимости в участии специалиста нет. Так, Московский городской суд указал, что телефон является средством мобильной связи, не предназначен исключительно для накапливания и хранения данных; в момент изъятия самого телефона снятие какой-либо содержащейся в нем информации не происходило, поэтому участия специалиста для изъятия телефона как предмета не требовалось[19].

Представляется, что указанное толкование закона противоречит императивной норме части 2 статьи 164.1 УПК РФ, безусловно требующей участия специалиста при изъятии в ходе производства любых следственных действий электронных носителей информации. Во-первых, крайне затруднительно заранее предположить, какие именно электронные носители информации могут быть обнаружены в ходе, например, обыска. В современном мире сложно себе представить людей и организации без каких-либо электронных (цифровых) гаджетов. Поэтому практически уверенно можно утверждать, что при выезде на место обыска будут обнаружены какие-либо электронные носители информации, изъятие которых без участия специалиста может повлечь необратимые последствия. Известны случаи, когда простое отключение компьютера от сети питания приводило к потере важнейших данных и разрушению файловой системы, восстановить которые без участия специалиста было невозможно. Во-вторых, довольно часто, особенно на первоначальных этапах расследования («по горячим следам»), бывает необходимо приступить к изучению содержания электронных доказательств в момент их обнаружения. И в этом случае также необходимо участие специалиста. И в-третьих, специалист может помочь изначально определить значимую для расследования информацию, содержащуюся на том или ином электронном носителе, отделить неохраняемую и охраняемую законом информацию (в частности, личную и иную информацию, доступ к которой должен быть санкционирован судом), скопировать ее и обеспечить целостность и сохранность скопированной информации, оказать содействие следователю при идентификации этой информации и правильному указанию электронного (цифрового) ее носителя в ходе составления протокола следственного действия.

[18] *Галяшина Е. И.* Судебная фоноскопическая экспертиза: проблемы диагностики аутентичности фонограмм // Вестник Университета имени О.Е. Кутафина (МГЮА). 2014. № 3. С. 26.

[19] Апелляционное определение МГС от 5 марта 2019 г. № 10-3033/2019 // СПС «КонсультантПлюс».

В этой связи правоприменителю необходимо обеспечить участие специалиста при изъятии любого электронного носителя информации в ходе производства любого следственного действия, а судам скорректировать практику применения уголовно-процессуального закона в соответствии с его буквальным толкованием.

4. Оценка достоверности электронных (цифровых) доказательств предполагает возможность их аутентификации и идентификации.

Взяв за основу определения вышеуказанных понятий применительно к электронному документу, данных Зайцевым П. П.[20], можно предложить понимать под аутентификацией возможность проверки целостности и неизменности содержания электронного (цифрового) доказательства, а под идентификацией — возможность установления источника (лица) происхождения электронного (цифрового) доказательства.

Следует согласиться с высказанным в литературе мнением о том, что установление подлинности источника электронного доказательства связано с проверкой первоисточника, на котором хранилась информация, сводящаяся к установке отсутствия внесений модификаций[21].

В контексте рассматриваемого вопроса заслуживают внимания положения статьи 8 Типового закона ЮНСИТРАЛ об электронной торговле, согласно которой если законодательство требует, чтобы информация представлялась или сохранялась в ее подлинной форме, это требование считается выполненным с помощью сообщения данных, если имеются надежные доказательства целостности информации с момента, когда она была впервые подготовлена в ее окончательной форме в виде сообщения данных или в каком-либо ином виде. С этой целью критерием оценки целостности является сохранение информации в полном и неизменном виде, без учета добавления любых индоссаментов и любых изменений, происходящих в обычном процессе передачи, хранения и демонстрации[22].

Оценивая достоверность электронных (цифровых) доказательств, следует принимать во внимание достижения современной криминалистики по установлению электронных следов. Опираясь на известное в трасологии понятие «дорожка следов», Вехов Е. Б. выводит понятие *«дорожка электронных следов»*, под которым понимается система последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора (-ов) связи от компьютера преступника до компьютера потерпевшего. Элементы «дорожки электронных следов» состоят из записей: — в файловой системе (реестры операционной системы и др.) компьютеров преступника и потерпевшего; — в памяти компьютера или аппарата связи преступника, содержащие сведения об отправленной в адрес потерпевшего компьютерной информации или сеансе работы в компьютерной системе; — в памяти коммутационного устройства контроля, авторизации и аутентификации абонентов в сети оператора (-ов) связи; — в системе учета данных для начисления платы за оказанные услуги связи и из других записей[23].

Очевидно, что в процессуальном плане вышеуказанные элементы «дорожки электронных следов» последовательно должны найти отражение в материалах уголовного дела либо в экспертном заключении, составленным по итогам компьютерно-технического исследования либо в заключении специалиста.

Анализ судебной практики показывает, что суды при оценке достоверности электронных

---

[20] *Зайцев П.* Электронный документ как источник доказательств // Законность. 2002. № 4. С. 40—44.

[21] *Янин М. Г., Кочедыкова К. М.* Проблемы сбора, проверки и оценки электронных доказательств в уголовном судопроизводстве // Управление в современных системах. 2019. № 2 (22). С. 29.

[22] Типовой закон ЮНСИТРАЛ об электронной торговле 1996 г. П. 1, 3 ст. 8 // СПС «КонсультантПлюс».

[23] Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / С. В. Зуев [и др.] ; отв. Ред. С. В. Зуев. М. : Юрайт, 2020. С. 96—97.

(цифровых) доказательств, в частности, используют тест «идентификации» указанных доказательств.

Так, гр-н С. был осужден за совершение преступления, предусмотренного ч. 2 ст. 205.2 УК РФ, то есть за публичные призывы к осуществлению террористической деятельности и публичное оправдание терроризма, совершенные с использованием информационно-телекоммуникационной сети «Интернет», путем размещения на своей странице «АС» в социальной сети «ВК» двух публикаций, которые он прокомментировал текстами, содержащими призывы к совершению террористических актов и оправдание террористической деятельности. Сам С. вину не признал, приводил доводы о том, что вмененные ему материалы и комментарии на его странице в социальной сети «ВК» могли быть размещены иными лицами без его ведома и участия. Суды первой и апелляционной инстанций с доводами подсудимого не согласились, поскольку представленные обвинением доказательства подтверждали виновность С. в совершении инкриминируемого ему преступления.

В частности, доказательствами, подтверждающими, что именно С. разместил на своей странице в социальной сети «ВК» материалы и комментарии, содержащие призывы к осуществлению террористической деятельности, явились:

— протокол оперативно-розыскного мероприятия «получение компьютерной информации», отражающим результаты исследования персональной страницы «АС» в социальной сети «ВК», в ходе которого установлено размещение на этой странице, открытой для всеобщего доступа, указанных в приговоре материалов;
— показаниями свидетеля под псевдонимом Ш. о знакомстве его с С. и посещении персональной страницы последнего в социальной сети «ВК», где он видел изображения мужчины на фоне флага «ИГ» с надписью «Трепещи, русня», сопровождавшиеся комментариями пользователя;
— протоколом осмотра телефона С., в котором зафиксирован международный идентификатор этого устройства (IMEI);
— сообщением ООО «ВК» о датах и времени начала сессий пользователя «АС» в социальной сети «ВК» на его странице, которые имели место в указанное в приговоре время;
— сообщением ПАО «МТС» о регистрации абонентского номера за С.;
— показаниями специалиста К., подтвердившего, что именно пользователь персональной страницы «АС» социальной сети «ВК» через устройство IMEI с сим-картой с номером, зарегистрированным в ПАО «МТС», осуществлял выходы на данную страницу в социальной сети «ВК» и имел возможность разместить указанные в приговоре публикации и комментарии к ним[24].

В указанном деле основным доказательством являлось электронное доказательство, а именно — электронный документ, представленный в виде скриншота персональной страницы подсудимого С. в социальной сети «ВК». Подсудимый оспаривал принадлежность размещенных на его странице материалов, содержащих призывы к осуществлению террористической деятельности. Иными словами, защита утверждала, что не С. являлся автором этих материалов и он не размещал их на своей странице в сети «ВК». Перед следствием стояла задача идентифицировать имеющееся электронное доказательство, то есть установить источник его происхождения. Была собрана вышеуказанная совокупность доказательств, оценив которую суд счел доказанным (достоверно установленным, вне всяких разумных сомнений) факт размещения именно С. на своей странице в социальной сети «ВК» материалов, из содержания которых следует, что С. совершил преступление, предусмотренное ч. 2 ст. 205.2 УК РФ.

По рассматриваемой категории уголовных дел, как следует из изученных судебных актов, ключевыми «идентифицирующими» проверяемое электронное доказательство являются такие доказательства, как показания специалистов

[24] Апелляционное определение Верховного Суда РФ от 26 ноября 2019 г. № 225-АПУ19-1 // СПС «КонсультантПлюс».

и показания свидетелей о знакомстве с подсудимым и/или осмотре его страницы в сети «Интернет» в режиме реального времени. Это дает основания для выделения в законе такого самостоятельного действия, как осмотр сетевых информационных ресурсов, о чем говорилось выше. В этой же связи следует коснуться аспекта допустимости полученного доказательства, принимая во внимание, что осмотр страницы в социальной сети осуществляется чаще всего оперативными сотрудниками в ходе проведения ОРМ «получение компьютерной информации» и отражается в соответствующем протоколе. В апелляционных жалобах защитники указывают, что на осмотр страницы необходимо получение согласия владельца страницы. Верховный Суд РФ с этим доводом не соглашается, указывая, что получение такого согласия Федеральный закон «Об оперативно-розыскной деятельности» (ст. 8) связывает с применением мер безопасности в отношении защищаемых лиц, но никак не в отношении обвиняемых в совершении преступлений террористической направленности[25].

Оценка электронных доказательств в практике российского уголовного судопроизводства, как видно в том числе и из приведенных выше судебных дел, является сложным, требующим знание специфики данных доказательств процессом. Использование электронных (цифровых) технологий в процессе совершения преступлений с каждым годом возрастает. В ответ на это государство все большему количеству объектов предоставляет режим уголовно-правовой охраны, о чем вносятся соответствующие изменения в уголовный закон. В последние годы увеличилось число составов преступлений, диспозиция которых предусматривает совершение преступлений с использованием информационно-телекоммуникационных статей. Обобщая судебную практику по делам о преступлениях, совершаемых с использованием компьютерных технологий, Владимирский областной суд в подготовленной им по итогам обобщения Справке справедливо указал, что компьютерные (информационные) технологии представляют собой процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, а уникальные технические возможности и огромный потенциал сети «Интернет» удобны для использования в криминальных целях[26]. Указанные обстоятельства влекут необходимость более детального и подробного анализа процесса сбора, проверки и оценки электронных (цифровых) доказательств.

БИБЛИОГРАФИЯ

1. *Бахтеев Д. В., Смахтин Е. В.* Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. УрГЮУ. — 2019. — № 6. — С. 61–68.
2. *Воронин М. И.* Недопустимая допустимость электронных доказательств. Судебная практика и пробелы в УПК // Уголовный процесс. — 2020. — № 10. — С. 46–55.
3. *Галяшина Е. И.* Судебная фоноскопическая экспертиза: проблемы диагностики аутентичности фонограмм // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2014. — № 3. — С. 15–26.
4. *Добровлянина О. В.* Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации // Пермский юридический альманах. — 2019. — № 2. — С. 641–649.
5. *Зайцев П.* Электронный документ как источник доказательств // Законность. — 2002. — № 4. — С. 40–44.
6. *Овсянников Д. В.* Электронное копирование информации в системе средств уголовно-процессуального доказывания // Правопорядок: история, теория, практика. — 2014. — № 2 (3). — С. 130–134.

[25] Апелляционное определение Верховного Суда РФ от 14 января 2020 г. № 225-АПУ19-4 // СПС «КонсультантПлюс».

[26] СПС «КонсультантПлюс».

7. Основы теории электронных доказательств: монография / под ред. С. В. Зуева. — М. : Юрлитинформ. — 2019. — 398 с.
8. *Першин А. Н.* Осмотр сетевых информационных ресурсов — новый вид следственного действия? // Российский следователь. — 2020. — № 1. — С. 13–16.
9. Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / С. В. Зуев [и др.] ; отв. Ред. С. В. Зуев. — М. : Юрайт, 2020. — 196 с.
10. *Янин М. Г., Кочедыкова К. М.* Проблемы сбора, проверки и оценки электронных доказательств в уголовном судопроизводстве // Управление в современных системах. — 2019. — № 2 (22). — С. 28–31.

Материал поступил в редакцию 19 декабря 2021 г.

REFERENCES (TRANSLITERATION)

1. Bahteev D. V., Smahtin E. V. Kriminalisticheskie osobennosti proizvodstva processual'nyh dejstvij s cifrovymi sledami // Rossijskij yuridicheskij zhurnal. UrGYuU. — 2019. — № 6. — S. 61–68.
2. Voronin M. I. Nedopustimaya dopustimost' elektronnyh dokazatel'stv. Sudebnaya praktika i probely v UPK // Ugolovnyj process. — 2020. — № 10. — S. 46–55.
3. Galyashina E. I. Sudebnaya fonoskopicheskaya ekspertiza: problemy diagnostiki autentichnosti fonogramm // Vestnik Universiteta imeni O. E. Кutafafina (MGYuA). — 2014. — № 3. — S. 15–26.
4. Dobrovlyanina O. V. Nekotorye aspekty o processual'nom iz»yatii (kopirovanii) elektronnyh nositelej informacii // Permskij yuridicheskij al'manah. — 2019. — № 2. — S. 641–649.
5. Zajcev P. Elektronnyj dokument kak istochnik dokazatel'stv // Zakonnost'. — 2002. — № 4. — S. 40–44.
6. Ovsyannikov D. V. Elektronnoe kopirovanie informacii v sisteme sredstv ugolovno-processual'nogo dokazyvaniya // Pravoporyadok: istoriya, teoriya, praktika. — 2014. — № 2 (3). — S. 130–134.
7. Osnovy teorii elektronnyh dokazatel'stv: monografiya / pod red. S. V. Zueva. M. : Yurlitinform. — 2019. — 398 s.
8. Pershin A. N. Osmotr setevyh informacionnyh resursov — novyj vid sledstvennogo dejstviya? // Rossijskij sledovatel'. — 2020. — № 1. — S. 13–16.
9. Elektronnye dokazatel'stva v ugolovnom sudoproizvodstve: uchebnoe posobie dlya vuzov / S. V. Zuev [i dr.] ; otv. red. S. V. Zuev. — M. : Yurajt, 2020. — 196 s.
10. Yanin M. G., Kochedykova K. M. Problemy sbora, proverki i ocenki elektronnyh dokazatel'stv v ugolovnom sudoproizvodstve // Upravlenie v sovremennyh sistemah. — 2019. — № 2 (22). — S. 28–31.