УДК 343.14
DOI 10.34822/2312-377X-2021-1-29-34

Усольцев Ю. М., Усольцева Н. А.
Usoltsev Y. M., Usoltseva N. A.

МЕТАДАННЫЕ ЭЛЕКТРОННОГО СООБЩЕНИЯ КАК ЭЛЕКТРОННОЕ ДОКАЗАТЕЛЬСТВО В УГОЛОВНОМ ПРОЦЕССЕ

METADATA OF ELECTRONIC MESSAGES AS ELECTRONIC EVIDENCE IN A CRIMINAL PROCESS

Дана характеристика служебной информации электронных сообщений как источника доказательств в уголовном процессе, представлен анализ направлений развития понятия доказательства, вопросов изъятия электронной информации, электронных сообщений в рамках существующих процессуальных действий, а также использования метаданных в процессе доказывания по уголовным делам.

The article provides a characteristic of the electronic information of electronic messages as a source of evidence in criminal proceedings, analyzes the development trends of the concept of evidence in criminal proceedings, examines the issues of withdrawing electronic information from electronic messages within the framework of existing procedural actions, studies the possibility of using metadata in the process of proving in criminal cases.

Ключевые слова: метаданные электронного сообщения, электронное сообщение, электронное доказательство, использование электронных доказательств в уголовном процессе.

Keywords: metadata of an electronic message, an electronic message, electronic evidence, the use of electronic evidence in criminal process.

Цифровая реальность и электронный обмен сообщениями повсеместно приходят в нашу жизнь, и право не становится исключением. Наоборот, право не только говорит и обсуждает возможности использования процессов цифровизации, но и создает допустимые и возможные условия применения цифровой реальности и электронного документооборота в разных сферах. В этом поистине мировом процессе Россия также находится в тренде и ведет активную проработку нормативных актов для полноценного включения в правовую среду понятий, условий и механизмов цифровизации, в том числе и тех, с которыми мы сталкиваемся каждый день и даже не замечаем этого.

Процессуальное право, в отличие от многих других отраслей, все указанные вопросы рассматривает более серьезно, так как рассмотрение происходит сразу в двух проекциях:

1) возможности использования цифровых технологий и электронного обмена данными в условиях организации самого процесса (судебного или досудебного);

2) возможности использования цифровых технологий и электронного обмена данными как доказательств.

Уголовно-процессуальное право не стало исключением и в первую очередь делает акцент именно на второй проекции – определении таких понятий как «электронное доказательство» и «электронное доказывание» [4, с. 74–84].

Уголовно-процессуальный кодекс РФ (далее – УПК РФ) [18] не содержит в себе такого понятия как «электронное доказательство», но в ст. 74 представлен полный перечень доказательств, и этот перечень, если он не будет дополнен, позволяет говорить об электронной форме уже названного письменного доказательства, или электронном носителе информации как вещественном доказательстве, однако не позволяет говорить об электронных доказательствах как самостоятельном виде доказательств [12].

Основная часть процессуального сообщества, занимающаяся исследованием электронных доказательств, считает, что к электронным доказательствам можно относить любую

хранимую в электронном виде информацию (ESI): электронные документы, электронные письма, электронные файлы, а также электронные записи и служебные отметки. Для таких доказательств не требуется выделять отдельного вида доказательств в их классификации, а можно представлять средства доказывания в ныне существующих категориях – как вещественные или иные доказательства [13, с. 253, 254 ; 9, с. 107].

По мнению других исследователей, в УПК РФ необходимо просто детализировать институт доказательств, закрепив в нем возможность представления сведений также и в электронном виде [14; 1]. Некоторые авторы серьезно ратуют за новый вид доказательств и предлагают ввести электронные доказательства в уголовный процесс именно в таком статусе [7, с. 30]. Однако следует понимать, что данная тема не так однозначна и нуждается в тщательном исследовании всех составляющих ее компонентов.

Жизненно необходимо понимание того, что электронное доказательство – это не только электронное письмо (его содержание), электронная версия документа или иное упрощенное восприятие этого понятия. Одним из самых серьезных электронных доказательств, зачастую не обличенных в форму электронного документа, будут электронные данные, формируемые за счет программного алгоритма [12].

Электронные данные и электронная информация являются элементами не реального мира, скопированными или созданными с электронными технологиями («апгрейд версия» печатной машинки), а элементами цифрового мира, подтверждающими нечто, что создано или произошло именно в том мире, пока не имеющем в реальном мире никакого выражения. Именно эти электронные данные и электронная информация являются уникальными электронными доказательствами.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [11] определяет электронное сообщение как информацию, переданную или полученную пользователем информационно-телекоммуникационной сети, а информационно-телекоммуникационную сеть как технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

На данный момент ст. 474.1 УПК РФ определила, что в уголовном судопроизводстве допустим электронный документооборот (подачи ходатайств, жалоб и т. д.), а также «электронные носители информации» как вещественные доказательства [15, с. 78–83].

Каждый раз, создавая и отправляя электронное сообщение, мы словно не осознаем, что создаем уникальные цифровые следы своей активности, и именно они являются метаданными: дата и время отправки, заголовок, адрес отправителя, адрес получателя, тип вложения, его объем и прочие характеристики, то есть информация, которая сопутствует содержанию. Метаданные содержат больше ценной информации, чем мы привыкли думать [17].

Электронное сообщение словно расслаивается на три составляющие:

1) конверт (транспортный контейнер или пакет), содержащий сообщение и прикрепленные файлы. Конверт (транспортный контейнер) может быть подписан электронной подписью;

2) техническая или служебная часть сообщения, содержащая информацию об отправителе, транспортное движение, служебные отметки программ, идентификатор сообщения и т. д.;

3) собственно само сообщение или вложения, содержащее некую информацию, адресованную получателю.

Или, как указано в RFC-822 [19], а позднее в RFC-2822 [20], почтовое сообщение состоит из конверта, заголовка и тела сообщения. Пользователь видит только заголовок и тело сообщения. Конверт используется только программами доставки. Заголовок всегда находится перед телом сообщения и отделен от него пустой строкой.

RFC-822 регламентирует содержание заголовка сообщения. Заголовок состоит из полей. Поля состоят из имени поля и содержания поля. Имя поля отделено от содержания символом «:». Минимально необходимыми являются поля Date, From, cc или To. Поле Date определяет дату отправки сообщения, поле From – отправителя, а поля cc и To – получателя(ей).

Поле Message-ID содержит уникальный идентификатор сообщения и используется программами доставки почты. Message-ID – это уникальный идентификатор сообщения, то есть идентификатор, генерируемый при выкладывании сообщения в канале во время сеанса связи [6].

Поле Subject определяет тему сообщения, Reply-To – пользователя, которому отвечают, Comment – комментарий, In-Reply-To – показывает, что сообщение относится к типу «В ответ на Ваше сообщение, отвечающее на сообщение, отвечающее ...» (фразы исключены RFC-2822), X-Special-action – поле, определенное пользователем, в стандарте не определено.

Кроме того, используются поля заголовков, которые не регламентированы в RFC-822. Так, первое предложение заголовка, которое начинается со слова From, содержит UUCP-путь сообщения, по которому можно определить, через какие машины сообщение «пробиралось». Поле Received содержит транзитные адреса почтовых серверов с датой и временем прохождения сообщения; IP-адрес (Internet Protocol Address) – уникальный идентификатор (адрес) устройства (обычно компьютера), подключенного к локальной сети и (или) к Интернет.

Служебная или техническая часть электронного сообщения – это уникальный цифровой след, с помощью которого можно доказать необходимые обстоятельства в рамках производства по уголовному делу, в том числе определить программное обеспечение, технические данные устройства, время создания и изменения информации. Данные сведения позволят идентифицировать участника, проверить алиби или подтвердить виновность.

Формально все метаданные можно разделить на несколько условных групп:

- описательные метаданные, используемые для идентификации и поиска информации;
- структурные метаданные (навигационные пути);
- административные метаданные (административные отметки, в том числе по правам на информацию).

Метаданные электронного сообщения могут быть описательными и административными одновременно, включены в заголовок сообщения. Отправитель и получатель воспринимают только необходимую составляющую метаданных в своих почтовых программах (просмотр таких данных можно делать через специальные программы или через возможности самого почтового ресурса, предлагающего просмотреть все элементы технических заголовков). Доступ к метаданным электронного сообщения помимо отправителя и получателя имеют почтовые провайдеры, а также правоохранительные органы при проведении расследования или оперативно-розыскных мероприятий. Именно по этой причине метаданные подлежат весьма длительному хранению, в том числе и в России, что исходит из требования Федерального закона от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [10].

Помимо этого, метаданные могут дать третьим лицам информацию о пользователе абсолютно разнообразного характера, например, версии ПО, точке входа (адреса, имена, телефоны, контакты и т. д.), предположения о способах функционирования, предположения об использовании неявных технологий.

Какие метаданные обычно передаются вместе с документами: общие данные; название редактора (например, Microsoft Office Word); дата и время создания; идентификатор пользователя из настроек редактора на момент создания; дата и время редактирования; идентификатор пользователя из настроек редактора на момент редактирования; дата последней печати документа; количество правок; общее время редактирования документа; данные, сохраняемые с примечаниями к тексту (дата создания примечания); идентификатор пользователя из настроек редактора на момент создания примечания; полная история редактирования; поля документа (название, тема, ключевые слова, комментарий, пользовательские поля, цифровые подписи на документе, макросы в документе) [16].

Метаданные могут описывать не только электронное сообщение или электронный документ, но и электронный информационный ресурс, в качестве чего понимается формализованное описание электронного информационного ресурса, используемое для его идентификации и категоризации при работе с большими совокупностями информационных ресурсов. В этой ситуации метаданные признаются метаописанием электронного информационного ресурса [5].

Оценивая метаданные как электронное доказательство, стоит остановиться на том, что метаданные – это порождение цифровой среды, и если рассматривать их как доказатель-

ство, то доказательственным значением будут обладать именно они, а не носитель (вещественное доказательство или иной документ), на котором они были представлены следователю или суду. Оценивая и классифицируя метаданные как электронное доказательство, нужно сразу исключить форму носителя, так как в этой ситуации она не имеет значения, но при этом можно остановиться на позициях:

- способа доступа к метаданным – локальный или удаленный (возможны оба варианта);
- характера доступа к метаданным – могут быть доступными, но только для специальных субъектов [2, с. 61–68].

Дифференциация следов как носителей информации, используемая сегодня в криминалистических учениях, не выходит за рамки материальной и идеальной классификации [3, с. 25]. Но если «электронные носители информации» укладываются в эту систему как материальные следы, то сама техническая информация, создаваемая цифровым пространством по поводу тех же электронных сообщений и в нем существующая – это более сложный вопрос. Получение такой информации для доказывания по делу возможно через:

- привлечение специалистов, которые работают с изъятой компьютерной техникой или почтовыми ящиками конкретных лиц;
- при обращении к провайдеру интернета, который способен через транспортные сети отследить сообщение и предоставить всю информацию;
- при обращении к оператору почтового сервиса, который может дать полную информацию по входящим и исходящим электронным сообщениям.

Для расшифровки полученных от оператора или провайдера данных следователю может понадобиться обращение к специалисту, так как они относятся по характеру происхождения к опосредованным данным и их исследование предполагает наличие специальных познаний [2, с. 61–68].

Уголовно-процессуальный закон предусматривает несколько процессуальных действий, связанных с обнаружением и изъятием информации, содержащейся на электронных носителях: в ходе осмотра (места происшествия или помещения, компьютера или смартфона как предметов); в ходе выемки информации, содержащейся на компьютере или смартфоне, проводимой в рамках обыска помещения или направленной непосредственно на поиск устройства; возможно применение контроля и записи переговоров, получение информации о соединениях абонентов и/или абонентских устройств в рамках запросов в компании, предоставляющих услуги доступа к Интернету.

В 2018 г. законодатель внес изменения в УПК РФ, исключив отдельный вид выемки – выемку электронных носителей информации, добавив ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», распространив таким образом возможность работы с информацией в электронном виде в рамках любых следственных действий.

Однако новое понятие «изъятие» не получило аутентичного толкования. Под изъятием по-прежнему следует понимать элемент уголовно-процессуального принуждения, реализуемый в рамках имеющихся следственных действий, вид которых определяет следователь (дознаватель) по своему усмотрению, руководствуясь основаниями и условиями, сложившимися в рамках расследования.

Также немаловажно отметить, что подготовка следователя не предполагает по умолчанию знания технической стороны изъятия электронной информации. Для преодоления этой проблемы необходимо разрабатывать методические рекомендации следователям, дознавателям, судьям по работе с электронной информацией, метаданными файлов и программным обеспечением. В настоящее время УПК РФ устанавливает лишь обязательное присутствие специалиста при изъятии электронной информации, оставляя при этом на следователя (дознавателя) необходимость контроля за действиями специалиста и оценку полученных доказательств в целом.

Еще одним немаловажным фактором следует указать запрет на изъятие электронных носителей информации по отдельным составам преступлений, если изъятие может привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, за исключением прямо предусмотренных в законе случаев.

В этой ситуации единственным возможным вариантом действий следователя (дознавателя) остается использование именно самой электронной информации, фиксируемой в ходе копирования или получения ответа по запросу, что подводит нас к выводу о необходимости детальной регламентации «электронного доказательства» и введения данной категории в УПК РФ.

Если по аналогии рассматривать другие процессы, например, арбитражный, то можно сделать вывод, что дискуссия об электронных доказательствах идет также давно и эффективно и уже нашла отражение в реальных решениях и практиках, в том числе и по вопросу о метаданных.

Так, при предъявлении в арбитражном процессе электронного документа как доказательства, его необходимо транспонировать в документ на бумажном носителе с обязательным распечатыванием всех служебных заголовков. Рациональнее данную информацию перепроверить через провайдера почты отправителя, то есть отправлялось ли вообще в такое-то время сообщение с таким ID, закреплено ли IP отправителя за его интернет-провайдером, назначался ли IP именно отправителю и т. д., и придать доказательству легитимный статус, удостоверив его надлежащим образом у нотариуса [8, с. 28–30].

Подводя итог исследованию следует отметить необходимость решения следующих задач:

- включить в состав доказательств в уголовном процессе понятие «электронное доказательство»;
- детально регламентировать свойства данного доказательства;
- разъяснить понятие «изъятие» электронной информации в уголовном процессе;
- ориентировать должностных лиц на работу с метаданными электронных сообщений участников уголовного процесса;
- разработать рекомендации по использованию полученной электронной информации в методике расследования и тактике проведения отдельных следственных действий.

Литература

1. Александров А. С., Кувычков С. И. О надежности «электронных доказательств» в уголовном процессе. // Библиотека криминалиста. 2013. № 5 (10). С. 76–84.

2. Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Рос. юрид. журн. 2019. № 6. С. 61–68.

3. Белкин Р. С. Курс криминалистики : учеб. пособие для вузов в 3 т. Т. 2. М. : Юристъ, 2001. 464 с.

4. Воронин М. И. Электронные доказательства в УПК: быть или не быть? // Lex russica. 2019. № 7. С. 74–84.

5. ГОСТ 7.70-2003. СИБИД. Описание баз данных и машиночитаемых информационных массивов. Состав и обозначение характеристик. М. : Изд-во стандартов, 2004. 52 с.

6. ГОСТ Р 58546-2019 (IEC/PAS 62264-6:2016). Интеграция систем управления предприятием. Ч. 6. Модель службы обмена сообщениями : нац. стандарт Рос. Федерации : утв. и введен в действие Приказом Росстандарта от 20.09.2019 № 734-ст. М. : Стандартинформ, 2019. 86 с.

7. Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательства в уголовном процессе России : моногр. М. : Юрлитинформ, 2011. 173 с.

8. Малинина Е. С. Электронное сообщение как доказательство по делу в арбитражном судопроизводстве // Администратор суда. 2009. № 2. С. 28–31.

9. Марфицин П. Г. Некоторые подходы к формулированию понятия «электронное доказательство» в уголовном судопроизводстве // Вестн. Нижегород. Акад. МВД России. 2017. № 3 (39). С. 106–109.

10. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» : федер. закон Рос. Федерации от 06 июля 2016 г. № 374-ФЗ : принят Гос. Думой Федер. Собр.

Рос. Федерации 26 июня 2016 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 29 июня 2016 г. // Рос. газ. 2016. 08 июля.

11. Об информации, информационных технологиях и о защите информации : федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 08 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июл. 2006 г. // Рос. газ. 2006. 29 июля.

12. Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дис. ... канд. юрид. наук. М., 2016. 158 с.

13. Балашов А. Н., Балашова И. Н., Бахтеев Д. В., Брановицкий К. Л., Вехов В. Б., Григорьев В. Н., Долганичев В. В., Зазулин А. И., Зайцев О. А., Зуев С. В., Максимов О. А., Медведева М. О., Овсянников Д. В., Овчинникова О. В., Пастухов П. С., Тушканова О. В. Основы теории электронных доказательств : моногр. М. : Юрлитинформ, 2019. 398 с.

14. Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // Седьмой Пермский конгресс ученых-юристов : сб. науч. ст. М. : Статут, 2017. С. 558–566.

15. Смахтин Е. В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Рос. юрид. журн. 2018. № 4. С. 78–83.

16. Смирнов В. Метаданные электронных документов. // ECM-Journal.ru. URL : https://ecm-journal.ru/post/ (дата обращения: 20.04.2021).

17. Смирнов С. Метаданные: цифровые следы, которые мы (почти) не замечаем // Теплица социальных технологий. URL: https://te-st.ru/2020/02/12/metadata/ (дата обращения: 10.04.2021).

18. Уголовно-процессуальный кодекс Российской Федерации : федер. закон Рос. Федерации от 18 дек. 2001 г. № 174-ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 05 дек. 2001 г. // Рос. газ. 2001. 22 дек.

19. RFC-822 : Standard for ARPA Internet Text Message. Revised by David H. Crocker, Dept. of Electrical Engineering, University of Delaware, Newark, DE. 1982. URL: https://www.w3.org/Protocols/rfc822/ (дата обращения: 06.04.2021).

20. RFC 2822 : Internet Message Format. Ed. P. Resnick. April 2001. URL: https://www.ietf.org/rfc/rfc2822.txt (дата обращения: 06.04.2021).