УДК 343.14
DOI: https://doi.org/10.17308/vsu.proc.law.2022.1/9043

О ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВАХ В ЗАРУБЕЖНОМ УГОЛОВНОМ ПРОЦЕССЕ

П. Н. Бирюков

Воронежский государственный университет

Поступила в редакцию 1 июня 2021 г.

Аннотация: *статья посвящена проблемам цифровых доказательств (далее – ЦД) в уголовном процессе. Автор анализирует зарубежные подходы к доказательству в электронной форме, рассматривает существующие подходы, выявляет проблемы использования ЦД в уголовном судопроизводстве.*
Ключевые слова: *цифровые доказательства, Интерпол, ЕС, США, допустимость доказательств в электронной форме.*

Abstract: *the article is devoted to the problems of digital evidence (hereinafter CD) in criminal proceedings. The author analyzes foreign approaches to proof in electronic form, examines existing approaches, identifies the problems of using CDs in criminal proceedings.*
Key words: *digital evidence, Interpol, EU, USA, admissibility of evidence in electronic form.*

В начале 2000-х гг. большое внимание уделялось юридической силе доказательств, полученных из источников в иностранном государстве[1]. В конечном итоге предлагаемые нами нормы вошли в новый УПК РФ (ст. 455). «Иностранные» доказательства в настоящее время стали легальной частью российского уголовного судопроизводства. Однако жизнь не стоит на месте. В последнее время ситуация осложнилась существованием доказательств в электронной форме. В связи с их использованием возникает много вопросов.

Обычно ЦД связывают с «компьютерными» преступлениями (неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ; нарушение правил эксплуатации средств хранения, обработки или передачи информации и т. д.). Однако ЦД могут использоваться для расследования любого вида преступлений. Так, электронная почта или записи мобильного телефона подозреваемых могут содержать информацию о преступном поведении субъектов, свидетельствовать о местонахождении конкретных лиц во время совершения деяния, об их отношениях с соучастниками и т. д.

[1] См.: *Бирюков П. Н.* Нормы международного уголовно-процессуального права в правовой системе Российской Федерации. Воронеж, 2000 ; *Его же*. Международное уголовно-процессуальное право и правовая система Российской Федерации (теоретические проблемы) : дис. … д-ра юрид. наук. Воронеж, 2001.

В российской науке проблеме ЦД стало уделяться большое внимание. Подчеркивается важность доказательств в электронной форме, исследуются способы их изъятия и сохранения, освещается проблема допустимости и т. д.[2] Вместе с тем имеют место и случаи негативного отношения к ЦД. К примеру, А. М. Баранов пишет: «Источником (носителем) доказательств (информации) в уголовном процессе всегда является человек. Доказательство-информация существует только в сознании человека, нет человека – нет информации. Следовательно, протоколы следственных действий, заключение эксперта (в виде документа), протокол судебного заседания, иные документы, вещественные доказательства будут не носителями (источниками) информации, а ХРАНИТЕЛЯМИ информации. В таком случае электронная среда (Интернет), электронные средства сохранения и передачи информации будут не вещественными доказательствами и не электронными доказательствами, а хранителями информации»[3].

Не вдаваясь в дискуссии, отметим, что в российской юриспруденции до сих пор не решены многие серьезные проблемы использования ЦД, в их числе: оформление и изъятие доказательств, тактика их предъявления, правильный подбор специалиста и т. д. Кроме того, снижает эффективность использования ЦД низкий уровень знаний сотрудников органов правопорядка и недостаточная грамотность судей и аппарата судов. В связи с этим представляет интерес зарубежный опыт, поскольку во многих странах устоялось законодательство о ЦД, есть и соответствующая практика на этот счет.

В иностранной науке теория электронных доказательств достаточно разработана. Под ними понимается информация, хранящаяся или передаваемая в двоичной форме, которую можно использовать в суде[4]. Правда, авторы в последнее время отмечают, что ЦД имеют тенденцию становиться более объемными, более сложными, легко изменяемыми, потенциально более доступными для всех лиц[5]. Соответственно, совер-

[2] См.: *Гаврилин Ю. В.* Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 47–48 ; *Костенко Р. И., Петрова О. А.* Проблемы изъятия электронных носителей информации в отечественном уголовном процессе // Юридический вестник Кубанского гос. ун-та. 2021. № 1. С. 62–72 ; Курс уголовного процесса / под ред. Л. В. Головко. М., 2021. С. 444 ; и др.

[3] *Баранов А. М.* Электронные доказательства : иллюзия уголовного процесса XXI в. // Уголовная юстиция. 2019. № 13. С. 67.

[4] См.: Interactive Tool for Ranking Digital Evidence Needs / by Brian A. Jackson, Dulani Woods. URL: https://www.rand.org/pubs/tools/TL175.html ; *Frieden J. D., Murray L. M.* The admissibility of electronic evidence under the federal rules of evidence // Richmond Journal of Law and Technology. 2011. XVII (2) ; *Galves F., Galves C.* Ensuring the admissibility of electronic forensic evidence and enhancing its probative value at trial // Criminal Justice Magazine, 2004. № 19 (1) ; *Garfinkel S. L.* Digital forensics research: The next 10 years // Digital Investigation, 2010. № 7. P. 64–73 ; и др.

[5] См.: *Ryan D. J., Shpantzer G.* Legal Aspects of Digital Forensics. URL: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf ; *Garrie D. B.,*

шенствуются и методы работы с ними. В зарубежной науке уже говорят о «компьютерной» или «цифровой криминалистике»[6].

В связи с этим необходимо исследовать наработанный за рубежом опыт.

Важную роль в разработке правил относительно ЦД играют международные организации. Так, в 2019 г. Интерпол провел первый онлайн-тренинг, посвященный электронным доказательствам[7]. Были выявлены основные проблемы, возникающие при получении доказательств в цифровом формате, в том числе из иностранных источников, а также выработаны рекомендации как законодательным, так и правоохранительным органам государств-членов.

Далеко вперед продвинулся в этом направлении и Евросоюз. Так, 17 апреля 2018 г. Еврокомиссия представила два законопроекта о совершенствовании трансграничного сбора электронных доказательств: Регламент о Европейских ордерах о производстве и сохранении электронных доказательств по уголовным делам[8] и Директиву о назначении законных представителей для целей сбора доказательств по уголовным делам[9].

Регламент направлен на введение альтернативного механизма международного сотрудничества и правовой помощи. В нем закреплены процедуры для быстрого, эффективного и действенного доступа к доказательствам, находящимся за границей. Европейский ордер на производство (European Production Order) и Европейский сохранный ордер (European Preservation Order) наделяют компетентные органы государств правом запрашивать напрямую у зарубежных поставщиков услуг связи доступ к электронным данным, необходимым для преследования указанных в Регламенте преступлений, вне зависимости от нахождения штаб-квартиры компании или места хранения информации. При этом запрошен-

Morrissy J. D. Digital forensic evidence in the courtroom : Understanding content and quality // Northwestern Journal of Technology and Intellectual Property. 2014. № 12(2). P. 121–128 ; *Goldfoot J.* The physical computer and the fourth amendment // Berkeley Journal of Criminal Law. 2011. № 16(1). P. 112 ; *Grimm P. D.* Authenticating digital evidence // GP Solo. 2014. № 31(5). P. 47–49.

[6] См.: *Reith M., Carr C., Gunsch G.* An examination of digital forensic models // International Journal of Digital Evidence. 2002 ; *Carrier B.* Defining digital forensic examination and analysis tools // International Journal of Digital Evidence. 2003. № 1 ; *Eoghan Casey* (ed.). Handbook of Digital Forensics and Investigation. Academic Press, 2009 ; *Carrier Brian D.* Basic Digital Forensic Investigation Concepts. 7 June 2006.

[7] URL: https://www.interpol.int/News-and-Events/News/2019/First-INTERPOL-fully-online-training-focused-on-digital-evidence

[8] Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. URL: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position

[9] Proposal for a Directive of the European parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings // COM/2018/226 final - 2018/0107 (COD).

ные сведения не могут использоваться для иных целей, чем указанные в Ордере, за исключением предотвращения непосредственной и серьезной угрозы безопасности государства или его существенным интересам, или для судебных разбирательств.

Срок исполнения Ордера – 10 дней; в неотложных случаях – 6 часов. Для сравнения – средний срок исполнения запроса в рамках процедур взаимной правовой помощи составляет до 10 месяцев.

В конце 2020 г. Комитет Европарламента по гражданским свободам согласовал окончательный текст Регламента. Согласно докладу Комитета, с судебными властями страны проживания гражданина, чьи права нарушены, больше не проводятся консультации. Не требуется и подтверждать приказы о предоставлении электронных доказательств, как это было первоначально предложено в проекте доклада. При этом «пострадавшее государство» не сможет блокировать незаконные запросы данных об иностранных гражданах. «Это особенно прискорбно, поскольку государство – член ЕС, в котором проживает пострадавший, обычно лучше всего может защитить его основные и процессуальные права». Обращалось внимание и на отсутствие защиты от так называемых «рыболовных экспедиций» (fishing expeditions). Речь идет о случаях, когда правоохранительные органы запрашивают огромные объемы данных без каких-либо оснований либо чтобы выявить доказательства, о существовании которых они ранее не подозревали. Предлагается закрепить «право поставщика услуг отклонить Ордер в случае, если он является «явно оскорбительным» либо не нацелен на конкретного человека или ограниченную группу лиц»[10].

Теперь что касается Директивы о назначении законных представителей для сбора доказательств по уголовным делам. В настоящее время в государствах ЕС существуют разные подходы к обязанностям поставщиков интернет-услуг в сфере уголовного судопроизводства. Фрагментация и мозаичность регулирования в разных странах ЕС создают правовую неопределенность в данной сфере. В результате на компании могут возлагаться различные (иногда противоречащие друг другу) обязательства в зависимости от того, предоставляют ли они свои услуги на национальном или трансграничном уровне, в пределах ЕС либо в третьи страны.

В странах ЕС существуют разные подходы на этот счет.

Так, в 2017 г. в Германии был принят Закон «Об обеспечении прав в соцсетях»[11], обязывающий провайдеров назначать в Германии лицо, уполномоченное получать запросы о предоставлении информации от правоохранительных органов. Закон предусматривает санкции в размере до 500 тыс. евро за отказ назначить представителя или ответить на запрос учреждения правопорядка. Предусмотрена также обязанность

[10] URL: https://edri.org/our-work/e-evidence-mixed-results

[11] Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG). URL: http://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html

провайдеров социальных сетей сообщать о незаконном контенте в Федеральное управление уголовной полиции. В 2021 г. принят Закон «О борьбе с правовым экстремизмом и преступлениями на почве ненависти»[12], который развивает положения закона 2017 г.

Меры аналогичного характера пока лишь обсуждаются в Италии[13]. Бельгия, напротив, не требует наличия представителя компании на ее территории, но стремится обеспечить соблюдение правил иностранными провайдерами через внутренние процедуры[14].

Чтобы устранить указанную мозаичность регулирования, Директива обязывает поставщиков услуг назначать специальное подразделение либо должностное лицо – законного представителя (legal representative) для получения и исполнения Ордера. Провайдеры должны иметь право выбирать, в какой стране ЕС они назначают своего законного представителя; государства не могут ограничивать этот выбор. Вместе с тем законный представитель должен быть учрежден в государстве, где поставщик услуг предоставляет услуги либо учрежден, либо где находится его офис. При этом принимается во внимание наличие «существенной связи» между государством ЕС и компанией. Для определения наличия «связи» применяют также Регламент 1215/2012 о юрисдикции, а также признании и исполнении судебных решений по гражданским и коммерческим делам[15]. В случае неисполнения Ордера в отношении нарушителей предложены штрафы в размере до 2 % от общего годового оборота за предыдущий финансовый год.

В конце 2020 г. Комитет Европарламента по гражданским свободам согласовал окончательный текст Директивы[16]. В этом случае особых проблем не возникло. Однако напомним, что Директива нуждается в имплементации на национальном уровне государствами ЕС; поэтому посмотрим, как они это воплотят в национальном правопорядке.

В целом, проекты документов ЕС сокращают сроки доступа к доказательствам и обеспечивают прямое сотрудничество с поставщиками услуг[17]. Провайдеры и лица, данные о которых запрашиваются, будут вправе рассчитывать на определенные средства правовой защиты. За-

[12] Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=%2F%2F%2A%5B%40attr_id=%27bgbl121s0441.pdf%27%5D

[13] URL: http://www.publicpolicy.it/wp-content/uploads/2016/03/Relazione-Franco-Roberti-Dna.pdf

[14] Court of Appeals of Antwerp, judgment of 15 November 2017/ URL: http://www.lesoir.be/124825/article/2017-11-17/la-justice-belge-condamne-skype-payer-une-amende-de-30000-euros

[15] Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32012R1215

[16] URL: https://www.europarl.europa.eu/doceo/document/A-9-2020-0257_EN.html

[17] См.: *Tinoco-Pastrana Á.* The Proposal on Electronic Evidence in the European Union. URL: https://eucrim.eu/articles/proposal-electronic-evidence-european-union-spain

креплены в документах ЕС и гарантии основных прав человека, включая права на защиту личных данных. В целом, как отмечается, правоохранительные органы перестанут зависеть от доброй воли IT-компаний[18]. Документы также облегчают доступ к ЦД, которые хранятся за пределами Евросоюза.

В 2019 г. Совет ЕС дал Еврокомиссии два мандата на ведение переговоров о заключении международных договоров: а) с США для облегчения доступа к ЦД, включая коллизионные правила и общие правила прямой передачи доказательств; б) с Советом Европы о присоединении к Дополнительному протоколу к Будапештской конвенции о киберпреступности 2003 г.[19] Переговоры пока идут с разной степенью успеха.

В декабре 2020 г. Европол, Евроюст и Европейская судебная сеть опубликовали Отчет о ситуации с цифровыми доказательствами в ЕС[20]. Отмечается, что трансграничный доступ к информации имеет первостепенное значение для расследования постоянно растущего числа расследований широкого спектра преступлений (экономические, оборот наркотиков, торговля людьми, киберпреступность, преступления сексуальной направленности). В отчете приводятся примеры успешных расследований и называются проблемы, существующие на национальном уровне в разных странах ЕС.

Большое внимание уделяется ЦД в США[21]. С конца 70-х гг. прошлого века нарабатывалась соответствующая практика. Первые судебные решения об использовании компьютерной информации требовали, чтобы для аутентификации ЦД имелись «всеобъемлющие основания».

Так, в деле US v. Scholle суд подчеркивал, что прокурор предоставил надлежащие основания, продемонстрировав, что компиляции компьютерной информации о наркотиках составлялись регулярно. Кроме того, были предоставлены исходники компьютерной программы и процедуры контроля ввода, которые обеспечивали высокую точность и надежность полученных данных[22]. В результате преступник был осужден, в том числе и на основании доказательств в электронной форме.

В 80-х гг. прошлого века суды разрешили использовать ЦД: электронную почту, цифровые фотографии, журналы транзакций банкома-

[18] e-Evidence for EU legal practitioners 2021-2022. URL: https://era-comm.eu-/e-evidence/

[19] URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/189

[20] SIRIUS EU. Digital evidence situation report - 2nd Annual report. URL: https://www.europol.europa.eu/publications-documents/sirius-eu-digital-evidence-situation-report-2nd-annual-report

[21] См.: Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence / by Sean E. Goodison Robert C. Davis, Brian A. Jackson. URL: https://www.rand.org/pubs/research_reports/RR890.html; Adams, Richard. The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. 2012

[22] US v. Scholle, 553 F.2d 1109 (8th Cir. 1977). URL: https://scholar.google.com/scholar_case?case=17443300475547536181&q=553+F.2d+1109&hl=en&as_sdt=2,5

тов, текстовые документы, истории мгновенных сообщений, файлы программ бухгалтерского учета, истории интернет-браузеров, базы данных, содержимое памяти компьютера, резервные копии, распечатки, треки глобальной системы позиционирования, журналы электронных дверных замков отеля и цифровые видео- или аудиофайлы[23].

Было выработано несколько правил относительно использования ЦД. В частности, участникам процесса предлагается продемонстрировать «надежность компьютерного оборудования», «способ, которым исходные данные были изначально введены», «меры, принятые для обеспечения точности введенных данных», «метод хранения данных и меры предосторожности, принятые для предотвращения их потери», «надежность компьютерных программ, используемых для обработки данных» и «меры, принятые для проверки точности программ»[24].

По мере того как суды стали более осведомленными о цифровых документах, они стали отказываться от высоких стандартов доказывания по соответствующим делам. Так, в деле US v. Vela было решено, что «компьютерные данные ... должны рассматриваться как любые другие записи»[25]. При этом суд сам определял, являются ли доказательства относимыми и подлинными, не являются ли они «слухами» (hearing) и достаточно ли будет копии электронного документа либо потребуется оригинал[26].

В то же время суды разных штатов по-разному трактовали ЦД в целях аутентификации, «правил наилучших доказательств» и т. д. ЦД также часто подвергались критике из-за легкости, с которой они могут быть изменены. Правда, в последнее время суды все чаще отклоняют аргументы такого рода[27]. Так, суд США постановил, что «факт возможности изменения данных, содержащихся в компьютере, явно недостаточен для установления ненадежности» (дело US v. Bonallo)[28].

Имелись трудности и при рассмотрении дел с участием суда присяжных. В связи с этим М. Маккаскер предупреждал: «Средний присяжный не имеет умение различать «хорошую науку» и «мусорную науку»; по-

[23] См.: *Hart A.* In court, digital evidence can shine or fizzle // The Atlanta Journal-Constitution. 2014, July 26 ; *Goodison S. E., Davis R. C., Jackson B. A.* Digital evidence and the U.S. criminal justice system. Research Report № RR-890-NIJ. Santa Monica, CA: RAND, 2015.

[24] См.: *Zupanec D.* Admissibility of Computerized Private Business Records // American law reports. 4th. cases and annotations. 1981. № 7. P. 16–19.

[25] US v. Vela, 673 F.2d 86, 90. URL: https://casetext.com/case/us-v-vela-2

[26] См.: *Casey E.* Digital Evidence and Computer Crime, Second Edition. Elsevier, 2004.

[27] *Ryan D. J., Shpantzer G.* Legal Aspects of Digital Forensics. URL: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

[28] United States *v. Bonallo*, 858 F.2d 1427, 1430-32 (9th Cir. 1998). URL: https://casetext.com/case/us-v-bonallo

этому суд должен помочь ему, исключив сомнительные доказательства» (Arizona v. Hicks)[29].

В декабре 2006 г. в рамках Федеральных правил гражданского судопроизводства[30] были введены в действие новые правила сохранения и раскрытия доказательств в электронном виде. Этот подход был перенят и в рамках уголовного процесса.

В настоящее время согласно Федеральным правилам доказывания США (в новой редакции)[31] нормы Правил применяются к ЦД аналогично традиционным документам.

Основная проблема, которая возникает с ЦД, – их допустимость[32]. В США электронные данные часто признаются судами недопустимыми, если они были получены без санкции суда. В большинстве штатов по-прежнему требуется ордер для изъятия и исследования цифровых устройств. Это может создать проблемы в расследовании, когда в процессе выявляются доказательства иных преступлений. Так, широко известно дело К. Шредера: при расследовании другого преступления следователи обнаружили на компьютере преступника порнографические изображения детей; чтобы предъявить ему обвинение по этому пункту, необходимо было получить второй ордер[33].

Другое дело иллюстрирует способы исследования ЦД. В частности, в 2008 г. большое жюри округа Орандж, штат Флорида, предъявило Кейси Энтони обвинение в убийстве его дочери Кейли[34]. Прокурор утверждал, что Энтони применил хлороформ к Кейли, а затем задушил ее, прикрыв рот и нос девушки. Далее преступник положил тело дочери в багажник машины, а затем выбросил его. Останки были найдены менее чем в миле от дома родителей Энтони. Эксперт дал показания в пользу обвинения, заявив, что кто-то искал слово «хлороформ» в общей сложности 84 раза на компьютере, изъятом из дома Энтони[35]. Эксперт также показал, что

[29] Arizona v. Hicks, 480 S. Ct. 321 (1987). URL: https://supreme.justia.com/cases/federal/us/480/321

[30] Federal Civil Procedure Rules. URL: https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-civil-procedure#:~:text=The%20Federal%20Rules%20of%20Civil,action%20and%20proceeding."%20Fed

[31] Federal Rules of Evidence 2020. URL: https://www.law.cornell.edu/rules/fre (составляют одну из федеральных частей «УПК США»).

[32] См. подробнее: *Бирюков П. Н.* О доказательствах в уголовном процессе США // Юридические стандарты государственной власти и правоохранительной деятельности : построение, организация, осуществление, эффективность : материалы Междунар. науч.-практ. конф., посвященной 100-летнему юбилею юрид. фак. Воронеж. гос. ун-та (Воронеж, 15–16 ноября 2018 г.) : в 2 ч. / под ред. Ю. Н. Старилова, О. С. Рогачевой. Воронеж, 2019. Ч. 2. С. 69–76.

[33] State v. Schroeder, 613 NW 2d 911 - Wis: Court of Appeals 2000. URL: https://cite.case.law/wis-2d/237/575

[34] Orange County, Florida On October 14, 2008, Casey Anthony. URL: https://en.wikipedia.org/wiki/Murder_of_Cooper_Harris#References

[35] См.: *Atkinson J. S.* Proof is not binary: The pace and complexity of computer systems and the challenges digital evidence poses to the legal system // Birkbeck Law Review 2014. № 2(2). P. 245–261.

при обыске была обнаружена часть разбитого жесткого диска компьютера, на котором, как предполагалось, хранились соответствующие файлы. Подразумевалось, что Энтони заранее провел эти поиски, что свидетельствовало о преднамеренности убийства и позволяло квалифицировать его как особо тяжкое. В то же время во время исследования компьютера эксперт использовал лишь два инструмента для поиска по ключевым словам, в ходе которого и было обнаружено слово «хлороформ». Хотя, как правило, «хорошей практикой» является дублирование результатов поиска с помощью нескольких инструментов.

В данном случае, как указывает К. Новак, «это вызвало путаницу у присяжных. Отметки времени, указывающие, когда был произведен конкретный поиск, не синхронизировались между двумя используемыми инструментами»[36]. Адвокат защиты увидел слабость в версии обвинения и обратил внимание присяжных. Он заявил, что данные «экспертизы, включающие исследования хлороформа, являются центральным элементом их аргумента преднамеренности; они были использованы, чтобы ввести в заблуждение присяжных, и что недостатки в этих доказательствах заразили все их дело, как рак»[37]. В итоге Энтони был признан невиновным по обвинению в убийстве первой степени, в том числе из-за недопустимости представленных ЦД. Это дело продемонстрировало значение электронной информации для уголовного судопроизводства.

Важна также и полнота ЦД. Так, по делу об убийстве Р. Харрисом своего сына в 2014 г.[38] экспертиза компьютера, мобильного телефона, флэш-накопителя, жесткого диска компьютера, SD-карт и DVD, принадлежащих обвиняемому, привели полицию к обнаружению мотива убийства. У сына Харриса был роман с 17-летним школьником. Восстановленные поисковые запросы в Интернете продемонстрировали, что Харрис искал информацию о «возрасте согласия» в штате Джорджия и «как выжить в тюрьме». В 2016 г. Харрис был осужден за убийство первой степени и приговорен к пожизненному заключению.

Как известно, ЦД редко имеют удобочитаемый формат. Это требует от органов правопорядка и судов дополнительных шагов для использования их в качестве доказательств. Требуется так называемая «распечатка материала» (printing out the material). Для этого в уголовном процессе США применяется «правило наилучшего доказательства» (the

[36] *Novak M.* Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration // Journal of Digital Forensics, Security and Law. 2020. Vol. 14, № 4. Article 3. P. 2–3.

[37] *Bagley W. A.* Don't be evil: The fourth amendment in the age of google, national security, and digital papers and effects // Albany Law Journal of Science Technology. 2011. № 21(1). P. 153–192.

[38] См.: *Rankin B.* Ross Harris' hot car murder appeal still a work in progress // The Atlanta Journal-Constitution. 2019. September 3 ; *Boone Ch., Rankin B.* Ross Harris defense reveals frustrations with judge in hearing for new trial // The Atlanta Journal-Constitution. 2020. December 14.

best evidence rule)[39]. Если участник процесса хочет привести в качестве доказательства документ, оригинал которого недоступен, он должен предоставить суду приемлемое объяснение, объясняющее отсутствие оригинала. Если документ получить невозможно и суд находит предоставленное оправдание приемлемым, стороне разрешается использовать «вторичные доказательства для подтверждения содержания документа и использовать его в качестве допустимого доказательства»[40]. Так, в деле Aguimatang v. California State Lottery суд рассмотрел вопрос о допустимости ЦД, заявив, что компьютерная распечатка не нарушает правила наилучшего доказательства, поскольку считается «оригиналом»[41].

В результате Правило 1001 (d) «Федеральных правил доказывания» было изложено в новой редакции: «Для информации, хранящейся в электронном виде, «оригинал» означает любую распечатку – или другой вывод, читаемый визуально, – если он точно отражает информацию. «Оригинал» фотографии включает негатив или оттиск с него».

«Дубликат» означает копию, созданную механическим, фотографическим, химическим, электронным или другим эквивалентным способом или методом, который точно воспроизводит оригинал» (Правило 1001 (e)). «Дубликат допустим в той же степени, что и оригинал, за исключением случаев, когда возникает серьезный вопрос о подлинности оригинала или если обстоятельства делают несправедливым признание дубликата» (Правило 1003).

Указанные положения дополняются Правилом 1004: «Оригинал не требуется, и другие доказательства содержания письма, записи или фотографии допустимы, если:

(a) все оригиналы потеряны или уничтожены, и не по вине сторонника, действующего недобросовестно;

(b) оригинал не может быть получен никаким доступным судебным процессом;

(c) сторона, против которой будет предложен оригинал, имела контроль над оригиналом; в то время было извещено посредством состязательных бумаг или иным образом, что оригинал будет предметом доказывания в суде или слушании; и не предъявляет его в суде или слушании; или же

(d) написание, запись или фотография не имеют непосредственного отношения к контрольному вопросу».

Исследователи отмечают, что сбор ЦД требует иного набора компетенций, чем те, которые требуются для сбора обычных вещественных до-

[39] См.: Evidence: The Best-evidence Rule. Law Library - American Law and Legal Information. Web Solutions LLC.; Blackstone's Criminal Practice / Hooper; Ormerod; Murphy; et al. (eds.). Oxford, 2008.

[40] URL: https://www.law.cornell.edu/wex/best_evidence_rule#:~:text=The%20best%20evidence%20rule%20applies,acceptable%20excuse%20for%20its%20absence

[41] Aguimatang v. California State Lottery (1991). URL: https://law.justia.com/cases/california/court-of-appeal/3d/234/769.html

казательств[42]. Обращается внимание, что существует множество методов извлечения ЦД с различных компьютерных устройств. Сами методы, а также устройства, на которых хранятся доказательства, быстро меняются. Сложной задачей является и сохранение ЦД: в отличие от вещественных доказательств, они могут быть изменены или удалены. Следователи должны иметь возможность подтвердить достоверность доказательства и предоставить документацию, подтверждающую их целостность. Следователям необходимо самим повышать компьютерную грамотность и привлекать специалистов и экспертов.

Таким образом, вопросы получения и использования ЦД находятся в фокусе внимания зарубежной юриспруденции. Очевидно, что отечественная наука должна внимательно изучить опыт международных организаций и иностранных государств, чтобы использовать его как при направлении запросов о правовой помощи, так и при получении ЦД для расследования уголовных дел без «иностранного элемента».

Библиографический список

Баранов А. М. Электронные доказательства : иллюзия уголовного процесса XXI в. // Уголовная юстиция. 2019. № 13. С. 63–69.

Бирюков П. Н. Нормы международного уголовно-процессуального права в правовой системе Российской Федерации. Воронеж : ВГУ, 2000. 228 с.

Бирюков П. Н. Международное уголовно-процессуальное право и правовая система Российской Федерации (теоретические проблемы) : дис. … д-ра юрид. наук. Воронеж, 2001. 368 с.

Бирюков П. Н. О доказательствах в уголовном процессе США // Юридические стандарты государственной власти и правоохранительной деятельности : построение, организация, осуществление, эффективность : материалы Междунар. науч.-практ. конф., посвященной 100-летнему юбилею юрид. фак. Воронеж. гос. ун-та (Воронеж, 15–16 ноября 2018 г.) : в 2 ч. / под ред. Ю. Н. Старилова, О. С. Рогачевой. Воронеж : Изд. дом ВГУ, 2019. Ч. 2. С. 69–76.

Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 47–59.

Костенко Р. И., Петрова О. А. Проблемы изъятия электронных носителей информации в отечественном уголовном процессе // Юридический вестник Кубанского гос. ун-та. 2021. № 1. С. 62–72.

Курс уголовного процесса / под ред. Л. В. Головко. 3-е изд. М. : Статут, 2021. 1328 с.

[42] См.: *Friess N.* When rummaging goes digital: Fourth amendment particularity and stored e-mail surveillance // Nebraska Law Journal. 2013. № 90(4). P. 972–1016 ; *Frost A.* Inferiority complex: Should state courts follow lower federal court precedent on the meaning of federal law? // Vanderbilt Law Review. 2015. № 68. P. 53–103 ; *Garfinkel S. L.* Digital forensics // American Scientist. 2013. № 101(5). P. 370 ; *Gershowitz A. M.* The post-riley search warrant: Search protocols and particularity in cell phone searches // Vanderbilt Law Review. 2016. № 69(3). P. 585–638.

References

Baranov A. M. Electronic evidence: the illusion of criminal procedure in the 21st century // Criminal Justice. 2019. № 13. P. 63–69.

Biriukov P. N. The norms of international criminal procedure law in the legal system of the Russian Federation. Voronezh : Voronezh State University, 2000. 228 p.

Biriukov P. N. International criminal procedural law and the legal system of the Russian Federation (theoretical problems) : diss. … Doctors of legal sciences. Voronezh, 2001. 368 p.

Biriukov P. N. On evidence in the US criminal process // Legal standards of state power and law enforcement: construction, organization, implementation, efficiency. Materials of the International Scientific and Practical Conference dedicated to the 100th anniversary of the Law Faculty of Voronezh State University (Voronezh, November 15–16, 2018) : in 2 p. / ed. Yu. N. Starilova, O. S. Rogacheva. Voronezh : Voronezh State University Publishing House, 2019. Part 2. P. 69–76.

Gavrilin Yu. V. Electronic data carriers in criminal proceedings // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2017. № 4 (44). P. 47–59.

Kostenko R. I., Petrova O. A. Problems of confiscation of electronic media in the domestic criminal process // Legal Bulletin of the Kuban State University. 2021. № 1. P. 62–72.

Course of criminal procedure / ed. L. V. Golovko. 3rd ed. M. : Statut, 2021. 1328 p.

Для цитирования:

Бирюков П. Н. О цифровых доказательствах в зарубежном уголовном процессе // Вестник Воронежского государственного университета. Серия: Право. 2022. № 1 (48). С. 275–286. DOI: https://doi.org/10.17308/vsu.proc.law.2022.1/9043

Recommended citation:

Biriukov P. N. On digital evidence in criminal foreign proceedings // Proceedings of Voronezh State University. Series: Law. 2022. № 1 (48). P. 275–286. DOI: https://doi.org/10.17308/vsu.proc.law.2022.1/9043

Воронежский государственный университет

Бирюков П. Н., доктор юридических наук, профессор, заведующий кафедрой международного и евразийского права

E-mail: birukovpn@yandex.ru

Voronezh State University

Biriukov P. N., Doctor of Legal Sciences, Professor, Head of the International and Eurasian Law Department

E-mail: birukovpn@yandex.ru