Право. Журнал Высшей школы экономики. 2021. Т. 14. № 5.
Law. Journal of the Higher School of Economics. 2021. Vol. 14, no. 5.

Научная статья
УДК 343+341.45
DOI: 10.17323/2072-8166.2021.5.236.255

Электронная информация по уголовным делам в рамках международного сотрудничества (правовая природа и классификация)

Кирилл Константинович Клевцов

Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Москва, Россия, klevtsov001@gmail.com, https://orcid.org/0000-0003-2918-175X

Аннотация

Статья посвящена теоретико-правовому исследованию такого многогранного явления, как «электронная информация». Целью является определение концепта, правовой природы и видов такой информации в контексте уголовного процесса. В ходе анализа использованы материалистическая диалектика, юридическая герменевтика (правовая экзегеза), специально-юридический, сравнительно-правовой методы, социологический и лингвистический подходы (компонентный анализ лексических значений и анализ переводческих трансформаций), а также метод прогнозирования. В процессе изучения показано, что в законодательстве, доктрине и правоприменительной практике отсутствует и до сих пор не сформирован единый подход к понимаю электронной информации по уголовным делам. Это связано с тем, что зачастую ее сравнивают с электронным доказательством, упуская при этом из виду ее уголовно-процессуальную природу. Автор приходит к выводу об отсутствии законодательного определения понятия «электронные доказательства» и возможности оперировать на сегодняшний день термином «электронная информация» с учетом его межотраслевого предназначения, соответственно, предлагается соответствующее определение указанного концепта. Кроме того, предпринята попытка определить виды электронной информации по уголовным делам, в том числе испрашиваемой в рамках международного сотрудничества в сфере уголовной юстиции, а именно, оказания взаимной правовой помощи. В качестве теоретической базы исследования послужили работы как отечественных, так и зарубежных юристов, а в качестве нормативной основы использованы как международные документы, так и законодательство Российской Федерации и ряда зарубежных государств. Немаловажным является и использование в качестве эмпирической базы исследования материалов

уголовных дел, в которых фигурировал феномен «электронная информация», а также сведений, содержащихся в Практическом руководстве по порядку запроса электронных доказательств из других стран, подготовленном совместно Управлением ООН по наркотикам и преступности, Исполнительным директоратом Контртеррористического комитета Совета Безопасности ООН и Международной ассоциацией прокуроров во взаимодействии с программами EuroMed Justice и Euromed Police.

Ключевые слова

уголовное судопроизводство, электронная информация, цифровая информация, компьютерная информация, электронные доказательства, международное сотрудничество, правовая помощь, экстерриториальность

Для цитирования: Клевцов К.К. Электронная информация по уголовным делам в рамках международного сотрудничества (правовая природа и классификация) // Право. Журнал Высшей школы экономики. 2021. № 5. С. 236–255. DOI: 10.17323/2072-8166.2021.5.236.255.

Research article

General Description of Electronic Information on Criminal Cases in the Framework of International Cooperation

Kyrill K. Klevtsov

Moscow State Institute of International Relations (University), Moscow, Russia. klevtsov001@gmail.com, https://orcid.org/0000-0003-2918-175X

Abstract

The article is devoted to theoretical and legal research of such a complex and multifaceted phenomenon as “electronic information”. The aim is to determine the concept, legal nature and types of such information in the context of the criminal process. The analysis used materialistic dialectics, legal hermeneutics (legal exegesis), special legal, comparative legal methods, sociological and linguistic approach (component analysis of lexical meanings and analysis of translation transformations), as well as the forecasting method. In the course of the study, it was shown that in the legislation, doctrine and law enforcement practice, there is no and still has not formed a unified approach to understanding electronic information in criminal cases. This is due to the fact that it is often compared with electronic evidence, while ignoring its criminal procedural nature. The author comes to conclusion that there is no legal legislative definition of the concept of “electronic evidence” and the possibility of operating with the term “electronic information” today, taking into account its cross-sectoral purpose, accordingly, an appropriate definition of this concept is proposed. In addition, an attempt was made to determine the types of electronic information on criminal cases, including those requested within the framework of international cooperation in the field of criminal justice, namely, the provision of mutual legal assistance, thereby such information takes on a supranational connotation. The works of both domestic and foreign lawyers served as a theoretical basis for

the study, and among the regulatory framework, both international documents and the national legislation of the Russian Federation and a number of foreign countries were identified. It is also important to use in this manuscript as an empirical basis for research the materials of some criminal cases in which the phenomenon of "electronic information" appeared, as well as the information contained in the Practical Guide on the procedure for requesting electronic evidence from other countries jointly prepared by the UN Office on Drugs and Crime, the UN Security Council Counter-Terrorism Executive Directorate and the International Association of Prosecutors in collaboration with EuroMed Justice and Euromed Police programs.

Keywords

criminal justice, electronic information, digital information, machine information, computer information, electronic evidence, international cooperation, legal assistance, extraterritoriality

For citation: Klevtsov K.K. General Description of Electronic Information on Criminal Cases in the Framework of International Cooperation. *Law. Journal of the Higher School of Economics,* 2021, no. 5, pp. 236–255. (In Russ.). DOI: 10.17323/2072-8166.2021.5.236.255.

Введение

На сегодняшний день на доктринальном уровне и у правоприменителей отсутствует четкое понимание феномена «электронная информация» и его места в системе права, в том числе в науках уголовно-правового цикла. Все это порождает серьезные трудности в использовании электронных данных в качестве доказательств по уголовным делам. Это вызвано отсутствием четкого восприятия всеобъемлющего термина «информация», которое также требует научного переосмысления на основе современных реалий.

Сегодняшнее время на доктринальном уровне определяется как информационное [Раенко С.И., 2013: 3]; [Idowu S.O., Capaldi N., Zu L., Gupta A.D., 2013: 5–7], поскольку информация (informatio)[1] интересна как ученым, так и обществу в целом. Однако до сих пор в философии и в других науках отсутствует единый подход к пониманию данного концепта. В связи с этим уместно утверждение В.М. Полонского, полагающего, что «состояние понятийно-терминологического аппарата науки позволяет судить о степени развития соответствующей ему теории, высветить различные стороны, отношения реальных объектов и многообразие познавательных задач…» [Полонский В.М., 1999: 16].

1. Общая характеристика концепта информации

Толковые словари русского языка определяют информацию, как: (1) сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством; и (2) сообщения, ос-

[1] Разъяснение, изложение (лат.)

ведомляющие о положении дел, о состоянии чего-нибудь [Ожегов С.И., Шведова Н.Ю., 2006: 250]. Подобное определение встречается и в словарях по юриспруденции [Борисов А.Б., 2010: 260].

Однако данный концепт рассматривается по-разному в зависимости от соответствующих направлений науки, что привело к отсутствую единого подхода к его формированию. На этот счет, как нам представляется, верно говорит В.Ф. Васюков, что подобная ситуация вызвана комплексным характером отношений, опирающихся на теоретические построения многих наук: информатики, теории связи, теории информации, кибернетики, философии, семиотики, информодинамики (науки об открытых информационных системах), информациологии (науки о получении, сохранении и передаче информации для различных множеств объектов) [Васюков В.Ф., 2020: 43–44].

В философии по общему правилу сформированы две теории — функциональная и атрибутивная. Под первой подразумевается тот факт, что информация является продуктом человечества, следовательно, познается только индивидуумом. Согласно второй концепции, она представляет собой материю наряду с пространством и временем [Урсул А.Д., 1975: 29]; [Жданко А.В., 2013: 238]. В то же время в информатике информация является первичным понятием по аналогии с «материей», «энергией», вследствие чего не может быть определена через простые категории, которые имеют четкие грани [Бауэр Ф.Л., Гооз Г., 1990: 18].

На сегодняшний день имеется законодательное определение рассматриваемого нами феномена. Согласно п. 1 ст. 2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» под ней понимаются сведения (сообщения, данные) независимо от формы их представления[2]. Вероятно, приведенная легальная дефиниция должна быть пересмотрена, поскольку, во-первых, с момента ее определения прошло немало времени и информация приобрела несколько иную форму, а во-вторых, эта дефиниция носит собирательный и в некотором роде расплывчатый характер.

2. Уголовно-процессуальная природа электронной информации

В уголовно-процессуальной науке также предпринимались попытки дать определение информации в контексте разработки теории доказательств. Так, например, В.Я. Дорохов подразумевал под ней «любые сведения, используемые как доказательство в уголовном процессе, имеющие сигнальную природу» [Дорохов В.Я., 1964: 110]. В то же время профессор А.А. Давлетов ука-

[2] СЗ РФ. 2006 № 31 (Часть I). Ст. 3448

зывал, что информация является элементом ретроспективного познания, средством, при помощи которого субъект познания устанавливает наличие или отсутствие факта [Давлетов А.А., 1991: 24]. Стоит разделить мнение А.И. Зазулина о том, что в уголовно-процессуальном и криминалистическом познаниях зачастую участники встречаются с аналоговой[3] или дискретной информацией[4], поскольку она сама воспринимается через опрос, показания участников, следы преступлений, а результаты обличаются либо в документах, содержащих результаты оперативно-разыскной деятельности, либо в протоколах следственных и судебных действиях [Зазулин А.И., 2018: 79].

2.1. Машинная, компьютерная и цифровая информация как смежные категории

Особую группу составляет электронная информация, которая имеет специфические черты, отличающие ее от обыденной. В ряде работ по уголовно-процессуальному праву, криминалистике и оперативно-розыскной деятельности встречаются схожие термины: «машинная информация», «компьютерная информация», «цифровая информация». Например, И.З. Карась под машинной информацией предлагает понимать информацию, циркулирующую в вычислительной среде, зафиксированную на физическом носителе, в форме, доступной восприятию ЭВМ, или передающуюся по телекоммуникационным каналам [Карась И.З., 1990: 40].

Следует отметить, что от оперирования приведенным выше термином в уголовно-правовых науках и в ходе борьбы с преступностью, по общему правилу, отказались. Это связано с использованием во многих правовых документах понятия «компьютерная информация»[5] или «компьютерные данные»[6].

---

[3] Аналоговым сигналом является речь человека или изображение на фотографии.

[4] Таковой является текст, состоящий из букв, символов.

[5] В силу п «б» ст. 1 Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, заключенного в Душанбе 28.09. 2018 (далее — Конвенция СНГ о компьютерных преступлениях) под последней разумеется информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи. См.: Информационный вестник Совета глав государств и Совета глав правительств СНГ. 2018. № 1 (37). С. 138–145. Примечание к ст. 272 УК РФ определяет ее как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Стоит обратить внимание и на недавно введенное оперативно-розыскное мероприятие — «получение компьютерной информации», предусмотренное п. 15 ст. 6 ФЗ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33. Ст. 3349.

[6] Пункт «b» ст. 1 Конвенции о преступности в сфере компьютерной информации ETS № 185, принятой в Будапеште 23.11.2001 (далее — Будапештская конвенция, Конвенция Совета Европы о компьютерных преступлениях), гласит, что «компьютерные данные означают

При этом, несмотря на имеющуюся международную легитимацию данного понятия, в научных кругах до сих пор идут дискуссии относительно его определения. Так, А.В. Касаткин полагает, что компьютерная информация — это фактические данные, которые обработаны компьютером и получены на выходе в форме, доступной восприятию ЭВМ или человеком [Касаткин А.В., 1997: 26]. В то же время В.В. Крылов под ней понимает сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях [Крылов В.В., 1997: 27]. Несколько расплывчатое определение дает Н.А. Зигура. По ее мнению, компьютерная информация представляет собой сведения, которые существуют в электронно-цифровой форме на материальном носителе [Зигура Н.А., 2010: 28].

Каждое из приведенных определений, несомненно, отражает те или иные характерные черты рассматриваемого нами феномена. Однако все же стоит указать на то, что понятие «компьютерная информация» применительно к наукам антикриминального цикла имеет некоторые отличительные признаки, которые, думается, необходимо учитывать при его определении.

В то же время следует задаться важным как с теоретической, так и практической точки зрения вопросом: информация, находящаяся в смартфонах, умных часах, планшетах, относится в юридическом смысле к компьютерной информации, хотя в обыденной жизни данные носители являются разновидностью компьютеров[7]. Неоднозначной информацией по своей правовой природе являются сведения, содержащиеся в цифровых фотоаппаратах, видеорегистраторах, в роботах-пылесосах и т.д.

К сожалению, российское законодательство однозначного ответа на данные вопросы не дает, что, полагаем, негативным образом сказывается в ходе правоохранительной деятельности, в том числе оперативно-разыскной и уголовно-процессуальной. К примеру, из-за отсутствия в Федеральном законе «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ раскрытия детально порядка оперативно-розыскных мероприятий и обилия документов закрытого характера в зависимости от оперативно-розыскного органа возникают трудности в получении информации, передаваемой по каналам систем мгновенных сообщений, а именно — с помощью какого вида оперативно-розыскного мероприятия такие данные можно получить? Посредством снятия информации с технических каналов связи (п. 11 ст. 6) либо получения компьютерной информации (п. 15 ст. 6)? На сегодняшний

любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнить ту или иную функцию» // СПС КонсультантПлюс.

[7] См.: понятие «компьютер». Available at: URL: https://ru.wikipedia.org/wiki/Компьютер (дата обращения: 01.12.2021)

день данный вопрос остается дискуссионным, несмотря на его регламентацию в отдельных ведомственных правовых актах. В связи с этим, к примеру, В.А. Мещеряков считает необходимым отказаться от термина «компьютерная информация», и предлагает заменить его на термин «электронно-цифровой объект» [Мещеряков В.А., 2004: 163].

Впрочем, некоторые ученые предлагают использовать формулировку «цифровая информация», принимая во внимание многообразие форм, в которых могут существовать и передаваться такие сведения [Walker C., 2001: 87–88]. Например, Н.И. Иванов полагает, что цифровая информация означает информацию, зафиксированную на машинных носителях, или передаваемую в пространстве в виде дискретных сигналов вне зависимости от их физической природы [Иванов Н.А., 2013: 97]. В свою очередь, С.П. Кушниренко под ней подразумевает информацию, представленную в виде последовательности цифр, доступную для ввода, обработки, хранения, передачи с помощью технических устройств [Кушниренко С.П., 2006: 43]. Некоторые ученые пошли дальше и предложили оригинальный термин, считая его аналогом цифровой информации. Это — «информация, представленная в электронном виде, которая зафиксирована на машинных носителях вне зависимости от их физической природы» [Кувычков С.И., 2016: 60].

Дабы не увязнуть в дискуссии по многочисленным частным вопросам данного понятия, целесообразно использовать более широкое и известное в правоприменительной деятельности по уголовным делам словосочетание «электронная информация». К примеру, в ст. 164[1] Уголовного процессуального кодекса Российской Федерации (далее — УПК РФ) говорится об особенностях изъятия электронных носителей информации и копирования с них информации при производстве следственных действий, а в ч. 7 ст. 185 УПК РФ используются термины «электронные сообщения», «сообщения, передаваемые по сетям электросвязи». На доктринальном уровне отмечается неоднозначность некоторых формулировок в данных статьях российского уголовно-процессуального закона [Васюков В.Ф., 2016: 15–18]; [Шайдуллина Э.Д., Шмелева О.Г., 2018: 44–49]; [Стельмах В.Ю., 2021: 146–155]. Следовательно, исходя из формальной логики, делается умозаключение, что данная информация является электронной. Заметим, что в научных кругах также оперируют данным концептом [Салиновский К.В., Маркелова Г.Ю., 2001: 18]; [Маслов А.В., Соскова К.А., 2017: 57–59]. Иностранные коллеги тоже в большинстве случаев выбирают подобный подход[8].

[8] См.: Уголовно-процессуальный кодекс Федеративной Республики Германии (Strafprozessordnung (StPO). Available at: https://www.gesetze-im-internet.de/stpo/; Уголовно-процессуальный кодекс Французской Республики // https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/ (дата обращения: 01.12.2021)

К электронной информации относятся различные файлы, которые содержат текст, фотографии, видеосъемку, звукозапись, в том числе передаваемую через систему мгновенных сообщений, базы данных и программы, системные файлы, служебные утилиты и протоколы их работы. При этом подобная информация может располагаться как физически на устройствах, так и удаленно (к примеру, в облачном хранилище данных — cloud storage)[9]. Очевидно, подобная электронная информация может быть использована в уголовно-процессуальном доказывании.

2.2. Электронная информация и электронные доказательства: равнозначные или диаметрально противоположные явления?

Одним из спорных также является вопрос о соотношении понятий «электронная информация» и «электронное доказательство». Прежде всего, это связано с не утихающими до сих пор дискуссиями о понятии доказательств [Вышинский А.Я., 1941]; [Полянский Н.Н., 1946]; [Владимиров Л.Е., 2000].

Впрочем, российский законодатель дал легальную дефиницию рассматриваемому феномену[10], заложив в него системный подход, состоящий из трех элементов: фактические данные (сведения о фактах); источники фактических данных; способы и порядок собирания, закрепления и проверки этих фактических данных (сведений о фактах) [Балакшин В.С., 2002: 31].

Сложнее обстоит дело с определением правовой природы электронных доказательств, о чем свидетельствуют в свою очередь доктринальная «палитра» мнений по этому поводу. Некоторые ученые отмечают, что доказательства, закрепленные в электронной форме, следует относить к традиционным видам доказательств. Например, С.П. Ворожбит в свете гражданско-процессуального права пишет, что «в зависимости от того, какие из данных, сохраненных в электронной форме, имеют доказательственное значение, т.е.

[9] Модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемая в пользование клиентам, в основном, третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, большой виртуальный сервер. Физически такие серверы могут располагаться удаленно друг от друга географически. Available at: URL: https://ru.wikipedia.org/wiki/ (дата обращения: 01.12.2021)

[10] Исходя из ч. 1 ст. 74 УПК РФ доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном УПК РФ, устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

содержат сведения, необходимые для установления обстоятельств дела, будет зависеть отнесение их к письменным, вещественным доказательствам, аудио- или видеозаписи» [Ворожбит С.П., 2011: 8].

Другие полагают, что электронные доказательства — особые группы в рамках уже существующих видов доказательств, вследствие чего их следует наделять специфическим статусом, принимая во внимание их сущностные признаки. К примеру, Ю.Н. Соколов предлагает закрепить в ст. 81 УПК РФ отдельно формулировку, позволяющую признавать вещественным доказательством также информацию, представленную в электронном виде, которая служила орудием преступления или сохранила на себе следы преступления, либо на которую направлены преступные действия [Соколов Ю.Н., 2010: 116]. Данная позиция является спорной, поскольку не демонстрирует отличий от действующей редакции приведенной статьи российского уголовно-процессуального закона (ст. 81).

Наконец, третья группа исследователей полагает, что электронные сведения — исключительно новый вид доказательств наряду с другими, закрепленными в ч. 4 ст. 74 УПК РФ, поскольку он обладает специфическими свойствами, которые делают его отличным от других видов доказательств [Зигура Н.А., Кудрявцева А.В., 2011: 30].

Заметим, что отечественная правоприменительная практика относит так называемые электронные доказательства к вещественным доказательствам, поскольку это напрямую предусмотрено ст. 81 и ст. 84 УПК РФ, вследствие чего мы разделяем позицию первой группы ученых, относящих их к традиционным видам доказательств.

Применительно к данной проблеме Р.И. Оконенко подметил, что, к примеру, при появлении в обществе фотоаппаратов, диктофонов и видеокамер, это не привело в следственно-прокурорской практике отнесения сведений, содержащихся в данных устройствах, к иному (особому) виду доказательств [Оконенко Р.И., 2016: 25]. Также это не вызвало появления новых следственных действий, которые позволяли получать такие экстраординарные доказательства. Стоит признать, что криминалистические особенности получения такой электронной информации, безусловно, имеются.

Об этом также показательно рассуждает профессор Л.В. Головко. По его мнению, если протоколы следственных и судебных действий будут составляться в электронной форме, то никакого нового «вида» доказательств здесь не будет, поскольку протоколы так и останутся протоколами вне зависимости от формы своего изготовления (рукописная, электронная и т.д.). В результате ученый приходит к мнению, что в специальных электронных доказательствах нет нужды [Головко Л.В., 2019: 22–25].

Возвращаясь к вопросу о терминологических аспектах двух поднятых ранее терминов, заметим, что некоторые международные документы оперируют

ют именно словосочетанием «электронные доказательства»[11]. В зарубежной доктрине подобная терминология также используется [Moussa A.F., 2021]; [Kerr O.S., 2005: 279]; [Mason S., 2014].

2.2.1. Опыт иностранных государств

Терминологическая «неразбериха» детерминирована различием подходов государств к определению в целом доказательств и их правовой природы. К примеру, в странах, входящих в группу англосаксонской правовой семьи (системы общего права), используется понятие доказательств в широком смысле, не вкладывая его отечественного процессуального оттенка, в результате чего к нему правомерно добавляется слово «электронные».

Так, в США отсутствует разграничение доказательств на виды, и в большей степени сделан акцент на формальных правах участников уголовного процесса при собирании и использовании в судах доказательств [Пицци У., 2019: 21–46]; [Бернам У., 2006: 207–216]; [Решетникова И.В., 1997]. Стоит подчеркнуть, что Федеральные правила о доказательствах США, являющиеся по сути фундаментальным документом по американскому доказательственному праву [Rothstein P.F., Raeder M.S., Crump D., 2012: 2], не содержат понятия «электронные доказательства», а используют словосочетание «информация, хранящаяся в электронной форме» (electronically stored information).

Как отмечает профессор О.А. Зайцев, в большинстве стран, входящих в романо-германскую правовую семью (система континентального права), допустимость использования электронной информации регламентируется общими положениями законодательства о традиционных доказательствах [Зайцев О.А., 2019: 50].

2.2.2. Оптимальный вариант

Не вдаваясь в серьезные размышления на этот счет, отметим, что на сегодняшний день в силу отсутствия нормативного и доктринального однозначного ответа на обозначенный выше вопрос следует использовать словосочетание «электронная информация», а не доказательства. В подтверждение этого вывода приведем позиции отечественных ученых в области уголовного процесса. Так, М.С. Строгович писал, что пока доказательство не закреплено процессуально, не стоит утверждать, что оно действительно суще-

[11] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final — 2018/0108 (COD). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri = COM%3A2018%3A225%3AFIN (дата обращения: 01.12.2021); Practical guide for requesting electronic evidence across borders. Vienna, 2019.

ствует [Строгович М.С., 1986: 302]. В то же время профессор С.А. Шейфер утверждал, что признать объект доказательством, ввести его в процесс является исключительно прерогативой органа предварительного расследования, прокурора и суда, поскольку именно решение о приобщении предмета или документа к делу представляет собой завершающий момент в формировании доказательства [Шейфер С.А., 1981: 45–46]. Примерно аналогичную позицию разделяют и другие ученые [Балакшин В.С., 2004: 94–109].

То же распространяется на сведения, полученные в рамках оперативно-разыскной деятельности по поручению следователя и дознавателя[12], а также в рамках проверки сообщения о преступлении (ст. 144 УПК РФ), которые могут считаться доказательством только после их «процессуальной оценки».

Рациональное зерно по данному вопросу содержится в рассуждениях Н.А. Зигуры, считающей, что представленная участниками уголовного процесса или иными лицами компьютерная информация «станет считаться доказательством» только после признания ее следователем относимой и допустимой, а это произойдет после воспроизведения, осмотра, составления протокола осмотра и удовлетворения ходатайства о приобщении носителя компьютерной информации к делу [Зигура Н.А., 2010: 131].

Отсюда следует: любая электронная информация, являющаяся *de facto* доказательством по уголовному делу, остается информацией, пока она не будет собрана, проверена и оценена по правилам российского уголовного судопроизводства (Раздел III УПК РФ «Доказательства и доказывание»). Тот же самый аргумент относится и к электронной информации по уголовным делам, полученной в рамках международного сотрудничества.

3. Виды электронной информации в контексте международного сотрудничества по уголовным делам

Определившись в общих чертах с терминологией и правовой природой электронной информации по уголовным делам, стоит перейти к еще одному интересному с теоретической точки зрения вопросу, не лишенному своего прикладного предназначения, — к вопросу о классификации указанных сведений. Данный вопрос нашел подробное урегулирование в рамках криминалистических исследований цифровых следов [Мещеряков В.А., 2002: 103]; [Волеводз А.Г., 2002: 159–161]; [Смушкин А.Б., 2012]; [Льянов М.М., 2020],

[12] В порядке, предусмотренном Приказами МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФГС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09. 2013 «Об утверждении инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или суд» // СПС КонсультантПлюс.

не затрагивая при этом вопросы получения электронной информации по уголовным делам в свете международного сотрудничества.

Итак, оставляя за скобками технические и криминалистические аспекты, предлагается следующая классификация приведенной выше информации.

В зависимости от этапов производства по уголовному делу: получение электронной информации в рамках досудебного производства (Часть 2 УПК РФ) и в ходе судебного производства (Часть 3 УПК РФ). При этом получение таких сведений в ходе досудебного производства может быть как в стадии возбуждения уголовного дела (Раздел VII УПК РФ), так и в период предварительного расследования (там же, раздел VIII)[13].

С учетом места ее хранения: a) информация, физически находящаяся в сети национальных серверов (национальные информационные ресурсы); (b) сведения, хранящиеся за рубежом (экстерриториальная информация).

По содержанию. Электронная информация может быть: (a) общедоступной; (b) конфиденциальной, т.е. содержать государственную или иную охраняемую законом тайну[14].

Применительно к правовой основе получения электронной информации. Она может быть истребована на основании: национального (внутригосударственного) законодательства[15] и/или норм международного права[16].

По субъектам. В зависимости от доступа к электронной информации такими могут быть: физические лица, располагающие электронным носителем информации[17], на котором подобные сведения хранятся и который имеет

---

[13] Исходя из предмета и целей исследования, автор рассматривает исключительно получение электронной информации в рамках досудебного производства по уголовным делам.

[14] В российском законодательстве к таким сведениям относятся: государственная тайна; коммерческая тайна; банковская тайна; служебная тайна; профессиональная тайна (к примеру, адвокатская, врачебная) и др. Указанная классификация вытекает из системного толкования положений УПК РФ, ФЗ «Об информации, информационных технологиях и о защите информации»; Закона РФ от 21.07.1993 № «О государственной тайне»; ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»; Трудовой кодекс Российской Федерации и законы о службе в правоохранительных органах; Гражданский кодекс Российской Федерации (например, ст. 857), ФЗ от 02.12.1990 № 395-1 «О банках и банковской деятельности», ФЗ от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации», ФЗ от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности», ФЗ от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации; Закон Российской Федерации от 02.07.1992 № 3185 «О психиатрической помощи и гарантиях прав граждан при ее оказании» [Попов Л.Л., 2010: 125–189].

[15] Например, ч. 4 ст. 21 УПК РФ, п. 3^1 ч. 3 ст. 10^1 ФЗ «Об информации, информационных технологиях и о защите информации».

[16] К примеру, в рамках Будапештской конвенции, Конвенции СНГ о компьютерных преступлениях и др.

[17] Подобная терминология закреплена на нормативном уровне (например, ст. 164^1 УПК РФ). Кроме того, по ГОСТу 2.051-2013 под электронным носителем понимается материаль-

доступ к ней; поставщик-услуг[18] либо представительство поставщика-услуг в другом государстве.

С учетом механизма получения таких сведений, можно поделить на электронную информацию, получаемую посредством: оперативно-розыскных средств, в том числе при международном полицейском сотрудничестве (к примеру, сотрудники оперативных подразделений направили запрос о содействии правоохранительным органам иностранных государств на основании межправительственных и межведомственных соглашений либо через Национальное центральное бюро Интерпола); следственных и иных процессуальных действий (например, через направление следователем запроса об оказании взаимной правовой помощи компетентным органам иностранного государства; самостоятельного предоставления необходимых сведений субъектом, имеющим физический или удаленный доступ к такой информации — поставщик-услуг либо владелец электронного носителя информации);в зависимости от уголовно-процессуальной судьбы электронной информации. Так, полученные в рамках международного взаимодействия данные могут быть признаны вещественными доказательствами (ст. 81 УПК РФ), так и в качестве иных документов (ч. 2 ст. 84 УПК РФ), либо не признаны таковыми, а при предоставлении электронных носителей информации возвращены обратно компетентным органам иностранного государства.

В рамках международного сотрудничества по уголовным делам, как правило, запрашиваются следующие виды электронной информации.

Основная (базовая) информация об абоненте (Basic Subscriber Information) указывает имя абонента (пользователя), а также может содержать сведения, как долго абонент использовал услугу и IP-адрес, с которого впервые был совершен вход в систему.

Информация о трафике (без информации о содержании) (Transactional Information), представляющая метаданные, связанные с оказанием услуг; включает: данные, касающиеся подключения, трафика или местоположения коммуникации (к примеру, IP-адрес или MAC-адрес); журналы регистрации доступа, в которых регистрируется время и даты доступа к услуге конкрет-

---

ный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. Электронные носители информации могут использоваться как самостоятельные объекты (флеш-накопители, карты памяти, различные съемные накопители, компакт-диск и т.п.), так и входить в состав различных объектов (серверов, системных блоков, ноутбуков, видеорегистраторов, планшетов, мобильных телефонов и т.п.). См. также: Информационное письмо Следственного комитета Российской Федерации 12.03.2019 № Исоп-226/2-8811-19 «Особенности применения статей 164 и 164[1] УПК РФ при производстве следственный действий».

[18] В настоящем исследовании под ним понимаются организации (компании), оказывающие услуги информационно-телекоммуникационной сети Интернет, кабельной сети, спутниковой сети, услуги социальный сетей и передающие информацию электронным способом.

ным физическим лицом, а также IP-адрес, с которого осуществляется доступ к услуге; журналы операций, в которых фиксируются продукты, полученные конкретным физическим лицом от поставщика или третьего лица (например, приобретение места в облачном хранилище).

Информация о содержании (content). Она составляет тело или текст электронного письма (сообщения), блога или поста, видео, изображения или звук, хранящиеся в цифровом формате (кроме данных об абоненте или метаданных) [Малов А.А., 2018: 57–58][19].

Так, в ходе уголовного преследования правоохранительными органами Франции террориста А., который убил двух офицеров французской полиции в их жилище, возникла необходимость в получении учетных записей злоумышленника социальной сети Facebook на смартфоне iPhone, который был изъят в рамках осмотра места происшествия. Одна учетная запись была создана на имя А., а вторая — на вымышленное имя, где преступник разместил видеоролик о двойном убийстве и сделал заявление об атаке.

Французские компетентные органы направили запрос об оказании взаимной правовой помощи в отношении информации о содержании обеих учетных записей Facebook правоохранительным органам США: поставщик услуг находится под юрисдикцией американских властей. Последние сообщили, что стандарт достаточного основания был соблюден только в отношении учетной записи на вымышленное имя ввиду размещения видеоролика об убийстве, но не в отношении личной учетной записи. Учетная запись на вымышленное имя имеет прямую связь с преступным деянием, тогда как у личной учетной записи такой связи нет[20].

Заключение

В правоприменительной практике и доктрине сформировались различные подходы к пониманию информации, которая представлена в электронной форме, и задействуется при раскрытии и расследовании преступлений. Для ее обозначения используются различные термины, а именно: «машинная информация», «компьютерная информация», «цифровая информация», «электронная информация», а в некоторой части — и «электронные доказательства». В силу отсутствия законодательного закрепления указанных по-

[19] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and 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. P. 43.

[20] Из архива автора.

нятий и единой точки зрения в науке относительно их правовой природы оперировать этими понятиями как состоявшимися категориями преждевременно. На сегодняшний день стоит исходить из более привычного и лаконичного термина — «электронная информация», поскольку именно он обладает всеми необходимыми функциональными признаками, учитывая при этом его многогранную уголовно-процессуальную сущность.

Под электронной информацией по уголовным делам (в широком смысле) предлагается понимать сведения, передаваемые посредством любых физических сигналов (как правило, в электронной форме), содержащиеся на соответствующих материальных (цифровых) носителях, т.е. в пригодном для восприятия человеком, и которые используются в ходе уголовного судопроизводства, в частности для установления обстоятельств, подлежащих доказыванию (ст. 73 УПК РФ). Вместе с тем следует учитывать также и классификацию электронной информации при раскрытии и расследовании преступлений в зависимости от: этапов производства по уголовному делу; месторасположения информации; содержания; правовой регуляция получения; обладателей; механизма предоставления; порядка использования. Относительно международного сотрудничества в сфере оперативно-разыскной деятельности и уголовного судопроизводства, как правило, запрашивается следующая электронная информация: базовая информация об абоненте; сведения о сетевых транзакциях; данные о содержании.

Список источников

1. Бауэр Ф.Л., Гооз Г. Информатика. Вводный курс. М.: Мир, 1990. 336 с.

2. Балакшин В.С. Доказательства в российском уголовном процессе: понятие, сущность, классификация. Екатеринбург: УрГЮА, 2002. 112 с.

3. Балакшин В.С. Доказательства в теории и практике уголовно-процессуального доказывания:. Екатеринбург: УМЦ УПИ, 2004. 298 с.

4. Борисов А.Б. Большой юридический словарь. М.: Книжный мир, 2010. 848 с.

5. Бернам У. Правовая система США. М.: Новая юстиция, 2006. 1216 с.

6. Васюков В.Ф. Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 15–18.

7. Васюков В.Ф. Теоретические и правовые аспекты расследования преступлений с использованием абонентской информации. Орел: Картуш, 2020. 340 с.

8. Владимиров Л.Е. Учение об уголовных доказательствах. Тула: Автограф, 2000. 464 с.

9. Ворожбит С.П. Электронные средства доказывания в гражданском и арбитражном процессе: автореф. дис. … к. ю. н. СПб., 2011. 235 с.

10. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 485 с.

11. Вышинский А.Я. Теория судебных доказательств в советском праве. М.: Юридическое изд-во, 1941. 248 с.

12. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 22–25.

13. Давлетов А.А. Основы уголовно-процессуального познания. Свердловск: Изд-во Уральского университета, 1991. 152 с.

14. Дорохов В.Я. Понятие доказательств в советском уголовном процессе // Советское государство и право. 1964. № 9. С. 108–117.

15. Жданко А.В. Введение в общую историологию. СПб.: Алетейя, 2013. 277 с.

16. Зайцев О.А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 42–57.

17. Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис.…к.ю.н. Екатеринбург, 2018. 251 с.

18. Зигура Н.А. Компьютерная информация как вид доказательства в уголовном процессе России: дис. … к.ю.н. Челябинск, 2010. 234 с.

19. Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательства в уголовном процессе России. М.: Юрлитинформ, 2011. 176 с.

20. Иванов Н.А. Цифровая информация в уголовном процессе // Библиотека криминалиста. Научный журнал. 2013. № 5. С. 93–102.

21. Карась И.З. Экономический и правовой режим информационных ресурсов // Право и информатика. 1990. № 2. С. 40–59.

22. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. … к.ю.н. М., 1997. 215 с.

23. Крылов В.В. Информационные компьютерные преступления. Учебное и практическое пособие. М.: Норма, 1997. 285 с.

24. Кушниренко С.П. Цифровая информация как самостоятельный объект криминалистического исследования // Вестник криминалистики. 2006. № 2. С. 43–47.

25. Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дис. … к.ю.н. Н. Новгород, 2016. 273 с.

26. Льянов М.М. Современный подход к классификации виртуальных следов // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 4. С. 47–55.

27. Малов А.А. Получение электронных доказательств от иностранных юрисдикций (на примере США) // Законность. 2018. № 9. С. 56–60.

28. Маслов А.В., Соскова К.А. Электронная информация как доказательство по уголовным делам // Центральный научный вестник. 2017. № 11. С. 57–59.

29. Мещеряков В.А. Электронные цифровые объекты в уголовном процессе и криминалистике // Воронежские криминалистические чтения. 2004. № 5. С. 153–169.

30. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронежского государственного университета, 2002. 407 с.

31. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80000 слов и фразеологических выражений. М.: ТЕМП, 2006. 944 с.

32. Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ: дис. ... к.ю.н. М., 2016. 158 с.

33. Полонский В.М. Понятийно-терминологический аппарат педагогики // Педагогика. 1999. № 8. С. 16–24.

34. Полянский Н.Н. Доказательства в иностранном уголовном процессе: вопросы и тенденции нового времени. М.: Юрид. изд-во, 1946. 142 с.

35. Пицци У. Судопроизводство без истины: почему наша система уголовного судопроизводства стала дорогой ошибкой и что нам необходимо сделать, чтобы восстановить ее. М.: Инфотропик Медиа, 2019. 280 с.

36. Попов Л.Л. Информационное право. М.: Норма, 2010. 495 с.

37. Раенко С.И. К вопросу о становлении информационного общества // Наука и современность. 2013. № 20. С. 189–194.

38. Решетникова И.В. Доказательственное право Англии и США. Екатеринбург: УрГЮА, 1997. 237 с.

39. Салиновский К.В., Маркелова Г.Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. 2001. № 6. С. 18–19.

40. Стельмах В.Ю. Необходимость изменения конструкции следственных действий, направленных на получение сведений, передаваемых по средствам связи // Вестник Санкт-Петербургского университета МВД России. 2021. № 1. С. 146–155.

41. Соколов Ю.Н. Информационные технологии в уголовном судопроизводстве. Екатеринбург: Телекоммуникационное право, 2010. 418 с.

42. Строгович М.С. Курс советского уголовного процесса: в 2-х томах. Т.1. М.: Наука, 1986. 470 с.

43. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–48.

44. Урсул А.Д. Проблема информации в современной науке. Философские очерки. М.: Наука, 1975. 287 с.

45. Шайдуллина Э.Д., Шмелева О.Г. Законодательное закрепление наложения ареста на электронную переписку в уголовном судопроизводстве // Вестник Дальневосточного юридического института МВД России. 2018. № 2. С. 44–49.

46. Шейфер С.А. Следственные действия. Система и процессуальная форма. М.: Юрлитинформ, 2001. 208 с.

47. Idowu S., Capaldi N., Zu L., Gupta A.D. Encyclopedia of Corporate Social Responsibility. Berlin: Springer, 2013. 2772 p.

48. Kerr O.S. Digital Evidence and the New Criminal Procedures. Columbia Law Review, 2005, vol. 105, pp. 279–318.

49. Mason S. Electronic evidence: dealing with encrypted data and understanding software, logic and proof. Journal of the Academy of European Law, 2014, vol. 15, pp. 25–36.

50. Moussa A.F. Electronic evidence and its authenticity in forensic evidence. Egyptian Journal of Forensic Sciences, 2011, vol. 11, pp. 1–20.

51. Rothstein P.F., Raeder M.S., Crump D. Evidence in a Nutshell: State and Federal Rules. Minneapolis: West Publishing Company, 2012. 816 p.

52. Walker C. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Crime Prevention and Community Safety, 2001, vol. 3, pp. 87–88.

References

1. Bauer F.L., Gooz G. (1990) *Computer science. Introductory course.* Moscow: Mir, 336 p. (In Russ.).

2. Balakshin V.S. (2002) *Evidence in Russian criminal procedure: concept, essence, classification.* Ekaterinburg: Ural State Law Academy, 112 p. (In Russ.).

3. Balakshin V.S. (2004) *Evidence in theory and practice of criminal procedural proof.* Ekaterinburg: Ural University, 298 p. (In Russ.).

4. Borisov A.B. (2010) Big law dictionary. Moscow: Knizhnyi mir, 848 p. (In Russ.).

5. Burnham U. (2006) *US legal system*. Moscow: Novaya justitsia, 1216 p. (In Russ.).

6. Davletov A.A. (1991) *Basics of criminal procedural knowledge.* Sverdlovsk: University, 152 p. (In Russ.).

7. Dorokhov V. Ia. (1964) The concept of evidence in Soviet criminal procedure. *Sovetskoe gosudarstvo i pravo* = Soviet State and Law, no. 9, pp. 108–117. (In Russ.).

8. Golovko L.V. (2019) Digitalization in Criminal Procedure: Local Optimization or Global Revolution? *Vestnik ekonomicheskoi bezopasnosti* = Herald of Economic Security, no. 1, pp. 22–25. (In Russ.).

9. Idowu S., Capaldi N., Zu L., Gupta A.D. (2013) Encyclopedia of Corporate Social Responsibility. https://doi.org/10.1007/978-3-642-28036-8_100896.

10. Ivanov N.A. (2013) Digital information in criminal proceedings. *Biblioteka kriminalista* = Library of Criminalist, no. 5, pp. 93–102. (In Russ.).

11. Karas' I.Z. (1990) Economic and legal regime of information resources. *Pravo i informatika* = Law and Informatics, no. 2, pp. 40–59. (In Russ.).

12. Kasatkin A.V. (1997) Collecting and using computer information in the investigation of crimes. Candidate of Juridical Sciences Thesis. Moscow, 215 p. (In Russ.).

13. Kerr O.S. (2005) Digital Evidence and the New Criminal Procedures. *Columbia Law Review*, vol. 105, pp. 279–318.

14. Krylov V.V. (1997) *Information computer crimes*. Moscow: Norma, 285 p. (In Russ.).

15. Kushnirenko S.P. (2006) Digital information as an independent object of forensic research. *Vestnik kriminalistiki* = Herald of Criminaltics, no. 2, pp. 43–47. (In Russ.).

16. Kuvychkov S.I. (2016). Use of information presented in electronic form in proving in criminal cases. Candidate of Juridical Sciences Thesis. Nizhny Novgorod, 273 p. (In Russ.).

17. L'ianov M.M. (2020) Modern classification of virtual traces. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniia* = Siberian Criminalistics Transactions, no. 4, pp. 47–55 (In Russ.).

18. Malov A.A. (2018) Obtaining electronic evidence from foreign jurisdictions (United States as a case). *Zakonnost'* = Legality, no. 9, pp. 56–60. (In Russ.).

19. Maslov A.V., Soskova K.A. (2017) Electronic information as evidence in criminal cases. *Tsentral'nyi nauchnyi vestnik* = Central Scholar Herald, no.11, pp. 57–59. (In Russ.).

20. Mason S. (2014) Electronic evidence: dealing with encrypted data and understanding soft-ware, logic and proof. *Journal of the Academy of European Law,* vol. 15, pp. 25–36.

21. Meshcheriakov V.A. (2004) Electronic digital objects in criminal procedure and forensic science. *Voronezhskie kriminalisticheskie chteniia* = Voronezh Criminalistics Transactions, no. 5, pp. 153–169. (In Russ.).

22. Meshcheriakov V.A. (2002) *Computer information crimes: theory and practice of investigation.* Voronezh: University, 407 p. (In Russ.).

23. Moussa A.F. (2021) Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences,* vol. 11, pp. 1-20. https://doi.org/10.1186/s41935-021-00234-6.

24. Okonenko R.I. (2016). Electronic evidence and ensuring rights of citizens to protect private life in criminal proceedings: a comparative analysis. Candidate of Juridical Sciences Thesis. Moscow, 158 p. (In Russ.).

25. Ozhegov S.I., Shvedova N. Yu. (2006) Explanatory dictionary of the Russian language. Moscow: Temp, 944 p. (In Russ.).

26. Polianskii N.N. (1946) *Evidence in foreign criminal proceedings: modern issues and trends.* Moscow: Yuridicheskoe izdatelstvo, 142 p. (in Russian);

27. Polonskii V.M. (1999) Conceptual and terminological apparatus of pedagogy. *Pedagogika* = Pedology, no. 8, pp.16–24. (In Russ.).

28. Pitstsi U. (2019) *Litigation Without Truth: Why Our Criminal Trial System Has Become a Costly Error and What We Need to Do to Rebuild It.* Moscow: Infotropik Media, 280 p. (In Russ.).

29. Popov L.L. et al. (2010) *Information Law*. Moscow: Norma, 495 p. (In Russ.).

30. Raenko S.I. (2013) Building information society. *Nauka i sovremennost'* = Science and Modernity, no 20, pp. 189–194. (In Russ.).

31. Reshetnikova I.V. (1997) *The law of evidence in England and the USA.* Ekaterinburg: Ural State Law Academy, 237 p. (In Russ.).

32. Rothstein P.F., Raeder M.S., Crump D. (2012) Evidence in a Nutshell: State and Federal Rules. Minnesota: West Publishing Company, 816 p.

33.Salinovskii K.V., Markelova G. Uu. (2001) Evidence-based value of electronic information in the Russian criminal process. *Rossiiskii sledovatel'* = Russian Investigator, no. 6, pp.18–19. (In Russ.).

34.Shaidullina E.D., Shmeleva O.G. (2018) Legislative consolidation of the seizure of electronic correspondence in criminal proceedings. *Vestnik Dal'nevostochnogo iuridicheskogo instituta MVD* = Herald of Far Eastern Law Internal Ministry Institute, no. 2, pp. 44–49. (In Russ.).

35. Smushkin A.B. (2012) Virtual traces in forensics. Zakonnost' = Legality, no. 8, pp. 43–48 (In Russ.).

36. Sheifer S.A. (2001) *Investigation. System and procedure.* Moscow: Yurlitinform, 208 p. (In Russ.).

37. Sokolov Yu. N. (2010) *Information technologies in criminal proceedings.* Ekaterinburg: Telekommunikatsionnoe pravo, 418 p. (In Russ.).

38. Stel'makh V. Yu. (2021) The need to change the design of investigative actions aimed at obtaining information transmitted by means of communication. *Vestnik Sankt-Peterburgskogo universiteta MVD* = Herald of Peterburg University of Internal Ministry, no. 1, pp. 146–155. (In Russ.).

39. Strogovich M.S. (1986) *Soviet criminal procedure*. Moscow: Nauka, 470 p. (In Russ.).

40. Ursul A.D. (1975) *Information in modern science. Philosophical essays.* Moscow: Nauka, 287 p. (In Russ.).

41. Vasiukov V.F. (2016) Some issues of conducting investigative actions aimed at detecting, fixing and seizure of electronic messages transmitted through mobile subscriber devices of cellular communication. *Rossiiskii sledovatel'* = Russian Investigator, no. 23, pp. 15–18. (In Russ.).

42. Vasiukov V.F. (2020) *Theoretical and legal aspects of crime investigation using subscriber information*. Orel: Kartush, 339 p. (In Russ.).

43.Vladimirov L.E. (2000) *Doctrine of criminal evidence.* Tula: Avtograf. 464 p. (In Russ.).

44. Vorozhbit S.P. (2011) Electronic means of evidence in civil and arbitration proceedings. Candidate of Juridical Sciences Thesis. Saint Petersburg, 235 p. (In Russ.).

45.Volevodz A.G. (2002) *Countering computer crimes: legal framework for international cooperation.* Moscow: Yurlitinform, 485 p. (In Russ.).

46. Vyshinskii A.Ya. (1941) *Theory of forensic evidence in Soviet law.* Moscow: Yuridicheskoe izdatelstvo, 248 p. (In Russ.).

47. Walker C. (2001) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. *Crime Prevention and Community Safety,* vol. 3, pp. 87–88.

48. Zaitsev O.A. (2019) Using electronic information as evidence in a criminal case: a comparative analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = Journal of Foreign Legislation and Comparative Law, no. 4, pp. 42–57. (In Russ.).

49. Zazulin A.I. (2018) Legal and methodological foundations for using digital information as proof in a criminal case. Candidate of Juridical Sciences Thesis. Ekaterinburg, 251 p. (In Russ.).

50. Zhdanko A.V. (2013) *Introduction to General Historiology.* Saint Petersburg: Aleteiya, 277 p. (In Russ.).

51. Zigura N.A. (2010) Computer Information as a type of evidence in criminal procedure in Russia. Candidate of Juridical Sciences Thesis. Chelyabinsk, 234 p. (In Russ.).

52. Zigura N.A., Kudriavtseva A.V. (2011) *Computer information as a type of evidence in the criminal process of Russia.* Moscow: Yurlitinform, 176 p. (In Russ.).

Информация об авторе:

К.К. Клевцов — кандидат юридических наук, доцент.

Information about the author:

K.K. Klevtsov — Candidate of Science (Law), Associate Professor.

Статья поступила в редакцию 10.09.2021; одобрена после рецензирования 22.11.2021; принята к публикации 29.11.2021.

The article was submitted 10.09.2021; approved after reviewing 22.11.2021; accepted for publication 29.11.2021.