УДК 343.14

К ПРОБЛЕМЕ ПРОЦЕССУАЛЬНОГО ОФОРМЛЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ПОЛУЧЕННОЙ ИЗ ИНТЕРНЕТ-ИСТОЧНИКОВ

С.В. Юношев, кандидат юридических наук, доцент, заведующий кафедрой «Уголовное право и процесс»
С.В. Кондратюк, преподаватель кафедры «Уголовное право и процесс»
Тольяттинский государственный университет, Тольятти (Россия)

Ключевые слова: уголовное судопроизводство; доказательственное значение; следственные действия; осмотр информационных объектов сети Интернет и сетевых каналов коммуникации.

Аннотация: Данная статья посвящена значимой проблеме уголовного судопроизводства – приданию доказательственного значения информации, полученной из информационных ресурсов. Показывается, что действующее отечественное уголовно-процессуальное законодательство никак не регламентирует особенности введения в доказательственную базу такой информации. Обосновывается тезис, что отсутствие надлежащей процессуальной регламентации существенным негативным образом сказывается на законности доказывания при расследовании и рассмотрении уголовных дел, на надежности и достоверности получаемых доказательств. При этом констатируется, что потребности правоприменительной практики настоятельно требуют восполнение существующего законодательного пробела, поскольку иное влечет угрозу признания полученных доказательств недопустимыми и, как следствие, прекращение уголовного преследования или постановление оправдательного приговора. Обращается внимание, что аналогичные процедуры уже известны и успешно функционируют в иных отраслях российского права, например, применительно к обеспечению доказательств нотариусами. В этой связи обосновываются предложения о введении дополнений в Уголовно-процессуальный кодекс РФ, направленные на введение нового вида осмотра, а именно осмотра информационных объектов сети Интернет и сетевых каналов коммуникации. Обосновываются существенные отличия предлагаемого следственного действия от традиционного осмотра предметов и документов, главным образом, в содержании протокола осмотра информационных ресурсов. Также рассматривается проблема предоставления следователю (дознавателю) от организации, предоставляющей услуги доступа к сети Интернет, информации персонального характера о пользователе сети. На основе анализа существующей следственной практики делается вывод о ее противоречии конституционным гарантиям на неприкосновенность частной жизни, установленным в ст. 23 Конституции РФ. Исходя из этого, предлагается законодательное закрепление возможности истребования такой информации лишь на основании судебного решения, получаемого в порядке ст. 165 УПК РФ.

ВВЕДЕНИЕ

На современном этапе развития информационного общества и телекоммуникационных технологий все чаще возникает необходимость придания информации из интернет-источников статуса доказательства в уголовном судопроизводстве. Между тем, при очевидной необходимости вовлечения подобной информации в орбиту уголовного судопроизводства [1], процессуальная регламентация процедуры ее получения и оформления, то есть по сути придания ей доказательственного значения, не отвечает современным потребностям [2]. В правоприменительной практике, при том, что доказывание в целом признается одной из основных проблем расследования и разрешения уголовных дел [3–5], тем не менее, давно разработаны и успешно функционируют алгоритмы придания доказательственного характера информации на бумажных носителях [6–8]. Однако, что касается электронных документов и иной информации, полученной из интернет-источников, то уголовно-процессуальное законодательство совершенно очевидно отстает от потребностей практики. Правоприменители в такой ситуации вынуждены работать в условиях неочевидности процессуальной регламентации, действовать на свой страх и риск, приспосабливая под нужды оперирования с электронными документами и интернет-информацией ту процессуальную регламентацию, которая для этого никак не приспособлена. Так, например, известно, что информацией об авторах и пользователях интернет-информации владеют организации, предоставляющие телекоммуникационные услуги. В условиях существующей процессуальной регламентации предоставление ими этих сведений, а также последующее использование полученной информации в качестве доказательств, вызывает обоснованные возражения с точки зрения устоявшихся представлений о допустимости и достоверности доказательств. В свою очередь, это приводит к утрате такой информацией доказательственного статуса, признанию доказательств недопустимыми и, как следствие, прекращению уголовного преследования или постановлению оправдательного приговора [9–11]. Исходя из изложенного, совершенствование порядка процессуального оформления как доказательства информации, полученной из интернет-источников, является насущной необходимостью.

Цель работы – выработка предложений, направленных на совершенствование процессуального порядка получения и процессуального оформления доказательственной информации из сети Интернет и от организаций, предоставляющих телекоммуникационные услуги.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

Авторы настоящей статьи едины во мнении, что в уголовно-процессуальном законодательстве России на сегодняшний день отсутствует надлежащий процессуальный порядок изъятия и процессуального оформления информации, полученной из сети Интернет.

Как известно, теорией и практикой уголовно-процессуального познания (доказывания) выработаны четыре критерия допустимости полученного по уголовному

делу доказательства: 1) доказательство должно быть получено уполномоченным на то субъектом (критерий надлежащего субъекта); 2) оно должно быть извлечено из надлежащего источника (например, недопустимо использование в качестве доказательства информации, полученной из анонимных источников); 3) требование законности способа получения доказательства (например, доказательство должно быть получено в ходе специально для этого приспособленного следственного действия); 4) требование надлежащего способа фиксации доказательства (например, отсутствие протокола следственного действия как основного способа фиксации его хода и результатов во всех случаях приводит к ничтожности полученных в ходе этого следственного действия данных) [12].

Что касается информации, хранящейся на информационных объектах сети Интернет (интернет-сайтах) либо сетевых каналах коммуникации (электронная почта, мессенджеры и др.), то названные выше критерии допустимости доказательств либо не работают, либо нуждаются в существенной трансформации применительно к рассматриваемой разновидности доказательств.

Так, в данном случае всегда возникает необходимость переноса электронного образа данной информации в привычный для уголовного судопроизводства формат материального носителя. Однако действующее уголовно-процессуальное законодательство не содержит достаточной регламентации этой процедуры, позволяющей осуществлять такой перенос с необходимыми для доказывания гарантиями надежности и достоверности.

Между тем, примеры законодательной регламентации подобных процедур с требуемыми гарантиями в иных отраслях права российского законодательства уже есть. Например, в соответствии со ст. 102 Основ законодательства Российской Федерации о нотариате по просьбе заинтересованных лиц нотариус обеспечивает доказательства, необходимые в случае рассмотрения дела в суде или административном органе, если имеются основания полагать, что представление доказательств впоследствии станет невозможным или затруднительным. В данном случае осуществляется нотариальное удостоверение интернет-страницы путем составления протокола, что может осуществляться и без извещения одной из сторон или заинтересованных лиц. Технология получения доказательства при этом содержит применение служебной программы «Tracert» [13; 14]. Полученная в результате этого нотариального действия распечатка свидетельствует, в частности, что осмотр указанного сайта произведен с данного сервера, а также, что в этой процедуре не были задействованы посторонние лица. В нотариально заверенном документе указываются: последовательность осмотра сайта; количество распечатанных экземпляров; вид распечатки сайта (цветной или черно-белый). Также в нотариальном документе обязательно фиксируются примененные технические средства и их характеристики: тип процессора; его оперативная память; программы осуществления доступа; провайдер и основание его деятельности. В завершение нотариусом удостоверяется, что протокол осмотра составлен в нескольких экземплярах, один из которых остается в деле у нотариуса, а остальные переданы заказчику.

Что касается уголовного судопроизводства, то проведенный анализ следственной практики показал, что если интересующая следствие интернет-информация находится в открытом доступе, то следственные органы, как правило, проводят осмотр интернет-страницы по правилам производства такого следственного действия как осмотр предметов и документов. Однако далеко не всегда должностные лица, проводящие данное следственное действие, указывают в протоколе необходимые сведения об интернет-документах, позволяющие впоследствии идентифицировать их и обеспечить надежную проверяемость полученной информации. Так, например, отчет трассировки с указанием времени ее производства составляется не всегда. Также не указываются ни последовательность осмотра интернет-страницы, ни сведения о количестве скриншотов, созданных при проведении осмотра, ни их содержание и наименование. Часто не указаны техническое устройство, с помощью которого произведен осмотр, его технические характеристики. К протоколу осмотра не приобщается дубликат страницы, путем ее перезаписи с помощью браузера на электронный носитель, с целью удостоверения информации, содержащейся на скриншотах. Вследствие этого, по нашему мнению, остается весьма спорным вопрос, обеспечивает ли необходимую доказательственную надежность получаемой информации производство такого следственного действия как осмотр предметов и документов в случаях, если предметом осмотра выступают информационные объекты сети Интернет.

Как уже указывалось, в настоящее время УПК РФ не регламентирует изъятие информации из сети Интернет либо с сетевых каналов телекоммуникации, которая находится в открытом доступе. Необходимое для этого процессуальное действие в УПК отсутствует. Предлагаем внесение дополнений в уголовно-процессуальное законодательство РФ путем добавления нового вида такого следственного действия как осмотр с установлением для него исчерпывающей процессуальной регламентации.

На сегодняшний день, как известно, законодательно выделяется целый ряд видов осмотра (ст. ст. 176, 178 УПК РФ), каждый из которых имеет свою собственную специфическую процессуальную регламентацию. Это: 1) осмотр места происшествия; 2) осмотр местности; 3) осмотр жилища; 4) осмотр иного помещения; 5) осмотр предметов и документов; 6) осмотр трупа. Кроме того, многие авторы правомерно указывают, что помимо этих видов осмотра «в сущности освидетельствование – это также разновидность осмотра» [15, с. 75], представляющая собой осмотр тела живого человека [16]. Помимо того, что осмотр является самостоятельным следственным действием, он выступает также неотъемлемой частью таких следственных действий, как: 1) наложение ареста на почтово-телеграфные отправления, их осмотр и выемка (ст. 185 УПК РФ); 2) контроль и запись переговоров (ст. 186 УПК РФ); 3) получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ).

И, тем не менее, очевидно, что ни один из существующих видов осмотра не приспособлен для придания доказательственного значения информации, хранящейся на информационных объектах сети Интернет

(интернет-сайты) либо сетевых каналах коммуникации (электронная почта, мессенджеры и др.).

Вследствие этого, нами предлагается законодательное закрепление новой разновидности осмотра – осмотра информационных объектов сети Интернет и сетевых каналов коммуникации.

Полагаем возможным предложить следующее содержание соответствующей нормы уголовно-процессуального права, закрепленной, например, в ст. 178.1 УПК РФ: «В целях обнаружения следов преступления в информационных объектах сети Интернет и сетевых каналах коммуникации, а также выяснения других обстоятельств, имеющих значение для уголовного дела, может быть произведен осмотр информационных объектов сети Интернет и сетевых каналов коммуникации».

При этом, по нашему мнению, настоятельной необходимостью является включение данного следственного действия в перечень тех видов осмотра, производство которых возможно до возбуждения уголовного дела (ч. 2 ст. 176 УПК РФ), поскольку именно та информация, что будет получена по результатам его проведения, как правило, и будет служить основанием для возбуждения уголовного дела [17].

Содержанием же данного следственного действия будет выступать осмотр интернет-страницы следователем с последующей фиксацией информации, имеющей значение для уголовного дела, на материальном носителе путем производства скриншотов.

Полагаем, что для производства осмотра информационных объектов сети Интернет и сетевых каналов коммуникации, находящихся в свободном доступе, вынесение следователем отдельного постановления в качестве юридического основания не требуется по аналогии с осмотром документов на бумажных носителях.

Если исследование не требует применения специальных знаний, то следователь (дознаватель) его производит единолично. При необходимости, к производству следственного действия может быть привлечен специалист соответствующего профиля.

По аналогии с ч. 1.1 ст. 170 УПК РФ полагаем, что участие понятых при производстве предлагаемого нами вида осмотра возможно по усмотрению следователя, но не является обязательным во всех случаях, поскольку, как того и требует ч. 1.1 ст.170 УПК РФ, его производство во всяком случае должно сопровождаться применением технических средств фиксации его хода и результатов.

Одним из существенных отличий предлагаемого следственного действия от осмотра предметов и документов должны выступать особенности его протоколирования. В протоколе осмотра информационных объектов сети Интернет и сетевых каналов коммуникации, помимо общих требований к содержанию протокола следственного действия (ст. 166 УПК РФ), обязательно должны отражаться: адрес исследуемой интернет-страницы; последовательность исследования; количество скриншотов, которые были получены при исследовании, а также их содержание.

Для производства данного следственного действия мы полагаем возможным применение служебной программы «Tracert» аналогично нотариальному порядку заверения скриншотов. Каждый скриншот должен содержать определенные реквизиты, позволяющие идентифицировать устройство, на котором они были произведены, время, дату, лицо, которое произвело исследование. Полученные скриншоты будут иметь процессуальный статус приложений к протоколу осмотра информационных объектов сети Интернет и сетевых каналов коммуникации.

Помимо изъятия цифровой информации из телекоммуникационных сетей в настоящее время существует проблема конечной персонализации пользователя в сети Интернет. В уголовно-процессуальном законодательстве РФ не регламентирован вопрос о предоставлении следователю (дознавателю) информации о конкретном пользователе, о контактах между пользователями социальный сетей, мессенджеров и иных сетевых каналов коммуникаций. Как известно, на серверах сетевых каналов коммуникации сохраняются данные об абоненте, о телекоммуникационном терминале, о начале и конце определенного соединения по дате и времени, объемах передаваемых данных и другие сведения о трафике. Очевидно, что вышеуказанные данные могут иметь важное доказательственное значение по уголовному делу. Например, согласно методическим рекомендациям по расследованию преступлений против половой неприкосновенности несовершеннолетних, совершенных посредством глобальной сети «Интернет» [18], следователю необходимо: произвести в организации, предоставляющей услуги доступа к сети Интернет, выемку информации о сетевой активности подозреваемого (обвиняемого), после чего осмотреть полученную информацию с участием специалиста; получить в компаниях-операторах сотовой связи информацию о соединениях между абонентами и абонентскими устройствами, в частности, находящимися в пользовании подозреваемого (обвиняемого), после чего произвести осмотр полученной информации; произвести выемку информации о регистрации и переписке подозреваемого (обвиняемого) на ресурсах «Вконтакте», «Рамблер Интернет Холдинг», «Мэйл.Ру» и других; произвести ее следственный осмотр.

По мнению отдельных авторов [19], а также исходя из смысла п. 11 Постановления Пленума Верховного Суда РФ от 01.06.2017 № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ), источником информации, получаемой в результате следственного действия, предусмотренного ст. 186.1 УРК РФ, могут выступать только базы данных операторов связи. Таким образом, учеными и практиками признается невозможным получение информации из других источников в рамках следственного действия, предусмотренного ст. 186.1 УПК РФ. Поскольку статьями 185 и 186.1 УПК РФ не регламентирован порядок получения информации об абонентах телекоммуникационных сетей, то в принципе невозможно и получение данной информации на законных основаниях.

Проведенный анализ следственной практики показал, что органы предварительного расследования в таких случаях предпочитают направлять в организации, предоставляющие услуги в области телекоммуникаций («Вконтакте», «Рамблер Интернет Холдинг», «Мэйл.Ру» и др.), запросы о предоставлении сведений о пользователях, их личных данных, об ip-адресах, с которых

осуществлялся вход, а также предоставлении истории их обращений. По нашему мнению, сложившийся порядок влечет существенное нарушение конституционных прав граждан, гарантированных ст. 23 Конституции РФ [20; 21]. В подобных случаях полагаем обязательным получение согласия суда на предоставление органам предварительного расследования такой информации. В связи с этим, для законного получения и дальнейшего использования информации, находящейся на серверах сетевых каналов коммуникаций, также необходимо внесение соответствующего дополнения в уголовно-процессуальное законодательство.

В связи с рассматриваемой проблематикой небезынтересным представляется обращение к международному опыту. Согласно §113a Закона о телекоммуникациях Федеративной Республики Германия от 22 июня 2004 года, поставщики общедоступных телекоммуникационных услуг обязаны хранить данные о трафике конечных пользователей. В соответствии с § 113b вышеуказанного закона эти поставщики хранят такие сведения как: адрес интернет-протокола, назначенный подписчику для использования в сети Интернет; уникальный идентификатор порта, используемого для доступа к сети Интернет и назначенного идентификатора пользователя; дата и время начала и окончания использования сети Интернет по назначенному адресу Интернет-протокола с указанием основного часового пояса. Согласно § 113c данного закона и §100a Уголовно-процессуального кодекса ФРГ по мотивированному приказу прокуратуры и с согласия суда поставщики общедоступных телекоммуникационных услуг предоставляют информацию о телекоммуникациях абонента, в том числе Интернет-трафик, в органы, осуществляющие уголовное преследование.

Исходя из международного опыта, полагаем, что уголовно-процессуальное законодательство России требует внедрения аналогичного способа получения правоохранительными органами информации подобного содержания, а также данных о трафике абонента. Это предложение может быть реализовано путем добавления в УПК РФ новой статьи 186.2 «Получение информации о сетевой активности пользователя в телекоммуникационных сетях». Она может быть изложена в следующей редакции: «При наличии достаточных оснований полагать, что информация о сетевой активности пользователя в телекоммуникационных сетях может иметь значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном статьей 165 УПК РФ». При этом к информации о сетевой активности пользователей в телекоммуникационных сетях должны быть отнесены любые действия лица, совершенные на телекоммуникационных ресурсах.

Получение такой информации, по нашему мнению, должно допускаться при производстве по уголовным делам о преступлениях средней тяжести, тяжких и особо тяжких. В ходатайстве следователя о производстве данного следственного действия, касающегося получения информации об активности пользователя в телекоммуникационных сетях, должны указываться: 1) уголовное дело, в рамках производства которого необходимо выполнить данное следственное действие; 2) основания, по которым производится данное следственное действие; 3) анкетные данные лица (при его наличии), в отношении которого производится данное следственное действие; 4) период, за который необходимо получить соответствующую информацию, и (или) срок производства данного следственного действия; 5) наименование организации, от которой необходимо получить указанную информацию.

При направлении такого ходатайства в организации, предоставляющие телекоммуникационные услуги, к данным об активности пользователя должны относится: идентификационный номер активного соединения или идентификационный номер конечного устройства; идентификационные личные данные пользователя при аутентификации, при мобильных соединениях, а также данные о местоположении пользователя; начало и окончание соответствующего соединения по дате и времени, объем передаваемых данных; конечные точки установленных соединений, их начало и окончание по дате и времени и, при необходимости, объем передаваемых данных; другие данные трафика, необходимые для создания и ведения учета в области телекоммуникаций и расчета затрат на предоставления этих услуг.

К необходимым данным об активности пользователя могут также относится: дата регистрации пользователя, личные данные пользователя, указанные при регистрации и последующие их изменения; идентификационные данные о сессиях пользователя, в требуемый период времени (ip-адреса, mac-адреса устройств); при возможности, отчет о месторасположении пользователя в определенном промежутке времени.

В случае принятия судом положительного решения о возможности получении информации о сетевой активности пользователя в телекоммуникационных сетях, его копия направляется следователем в соответствующую организацию. К таким организациям относят как организации, предоставляющие услуги доступа к сети Интернет, так и организации, предоставляющие доступ к социальным сетям, мессенджерам и т. п. Организация – адресат требования о предоставлении информации – должна предоставить ее путем фиксации на любом материальном носителе. Указанная информация предоставляется в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и сведения о лицах, чьи сообщения были предоставлены.

Следователь осматривает представленные документы, содержащие информацию об активности пользователя в телекоммуникационных сетях, о чем составляет протокол, в котором должна быть указана та часть информации, которая, по мнению следователя, имеет отношение к уголовному делу. Лица, присутствовавшие при составлении протокола, вправе изложить свои замечания или дополнения.

Представленные носители информации, содержащие сведения об активности пользователя в телекоммуникационных сетях, приобщаются к материалам уголовного дела в полном объеме на основании постановления следователя и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

ВЫВОДЫ

Из сказанного можно сделать вывод, что действующее уголовно-процессуальное законодательство России не содержит надлежащей регламентации порядка изъятия и процессуального оформления информации, полученной из сети Интернет, что вызывает существенные затруднения среди правоприменителей и сложности в доказывании.

Для устранения данного пробела правового регулирования с учетом имеющегося международного опыта предлагается внесение дополнений в действующий Уголовно-процессуальный кодекс РФ, связанных с выделением самостоятельного вида осмотра – осмотра информационных объектов сети Интернет и сетевых каналов коммуникации.

Также предлагается установить судебный порядок получения информации о сетевой активности пользователя в телекоммуникационных сетях, гарантирующий реализацию положений ст. 23 Конституции РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Петрухин И.Л. Теоретические основы реформы уголовного процесса в России. Ч. I. М.: ТК Велби, 2004. 224 с.
2. Шейфер С.А. Собирание доказательств по уголовному делу: проблемы законодательства, теории и практики. М.: Норма, 2015. 112 с.
3. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. М.: НОРМА-ИНФРА-М, 2012. 240 с.
4. Лазарева В.А. Доказывание в уголовном процессе. 5-е изд., перераб. и доп. М.: Юрайт, 2014. 359 с.
5. Белкин А.Р. Теория доказывания. М.: НОРМА, 1999. 429 с.
6. Борисевич Г.Я. Документы как доказательства в российском уголовном процессе // Вестник Пермского университета. Юридические науки. 2012. № 1. С. 202–216.
7. Локк Р.Г.-В. Истребование письменных документов и носителей информации в ином виде на стадии возбуждения уголовного дела // Актуальные проблемы борьбы с преступностью. Саратов: СЮИ МВД России, 2007. С. 113–126.
8. Сазонова Т.П. Истребование предметов и документов как способ собирания доказательств // Вестник Южно-Уральского государственного университета. Серия: Право. 2009. № 19. С. 48–51.
9. Уголовно-процессуальное право. Актуальные проблемы теории и практики / под ред. В.А. Лазаревой, А.А. Тарасова. 3-е изд., перераб. и доп. М.: Юрайт, 2016. 465 с.
10. Некрасов С.В. Юридическая сила доказательств в уголовном судопроизводстве. М.: Экзамен, 2004. 128 с.
11. Васяев А.А. Признание доказательств недопустимыми в ходе судебного следствия в суде первой инстанции в российском уголовном процессе. М.: Волтерс Клувер, 2010. 176 с.
12. Уголовный процесс / под ред. В.А. Лазаревой. М.: ЮСТИЦИЯ, 2017. 654 с.
13. Лебедев А. Нотариусы на защите прав в интернет: обеспечение доказательств нотариусами // Петербургский Нотариус. 2017. № 2. С. 3–4.
14. Шидловская Ю.В. Некоторые проблемные вопросы, связанные с производством осмотра информационного ресурса // Правовые проблемы укрепления российской государственности: сборник статей. Ч. 55. Томск: Том-кий ун-т, 2012. С. 137–139.
15. Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение. Самара: Самарский университет, 2004. 228 с.
16. Россинский С.Б. Следственные действия. М.: Норма, 2018. 240 с.
17. Олиндер Н.В. Типичные способы совершения преступлений с использованием электронных платежных средств и систем // Эксперт-криминалист. 2014. № 1. С. 13–15.
18. Методические рекомендации по расследованию преступлений против половой неприкосновенности несовершеннолетних, совершенных посредством глобальной сети «Интернет» / под ред. А.М. Багмета. М.: Академия Следственного комитета Российской Федерации, 2016. 73 с.
19. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами // Lex Russica. 2017. № 3. С. 141–153.
20. Гонтарь С.Н., Уваров Н.А. Развитие конституционного права лица на неприкосновенность частной жизни в сфере уголовного судопроизводства в новейшей истории // Вестник Университета. 2014. № 13. С. 290–292.
21. Аберхаев Э.Р. Право на неприкосновенность частной жизни: юридическая характеристика и проблемы реализации // Актуальные проблемы экономики и права. 2008. № 1. С. 90–94.

REFERENCES

1. Petrukhin I.L. *Teoreticheskie osnovy reformy ugolovnogo protsessa v Rossii* [Theoretical foundations of the reform of the criminal process in Russia]. Moscow, TK Velbi Publ., 2004. 224 p.
2. Sheyfer S.A. *Sobiranie dokazatelstv po ugolovnomu delu: problemy zakonodatelstva, teorii i praktiki* [Collection of evidence on a criminal case: the problems of legislation, theory, and practice]. Moscow, Norma Publ., 2015. 112 p.
3. Sheyfer S.A. *Dokazatelstva i dokazyvanie po ugolovnym delam: problemy teorii i pravovogo regulirovaniya* [Evidence and proof in criminal cases: problems of theory and legal regulation]. Moscow, NORMA-INFRA-M Publ., 2012. 240 p.
4. Lazareva V.A. *Dokazyvanie v ugolovnom protsesse* [Proving in criminal proceedings]. 5th izd., pererab. i dop. Moscow, Yurayt Publ., 2014. 359 p.
5. Belkin A.R. *Teoriya dokazyvaniya* [Theory of proof]. Moscow, NORMA Publ., 1999. 429 p.
6. Borisevich G.Ya. Documents as proofs in the Russian criminal procedure. *Vestnik Permskogo universiteta. Yuridicheskie nauki*, 2012, no. 1, pp. 202–216.
7. Lokk R.G.-V. Vindication of written documents and other data carriers at the stage of initiation of a criminal case. *Aktualnye problemy borby s prestupnostyu*. Saratov, SYuI MVD Rossii Publ., 2007, pp. 113–126.
8. Sazonova T.P. Vindication of items and documents as a manner of collecting evidences. *Vestnik Yuzhno-*

Uralskogo gosudarstvennogo universiteta. Seriya: Pravo, 2009, no. 19, pp. 48–51.
9. Lazareva V.A., Tarasova A.A., eds. *Ugolovno-protsessualnoe pravo. Aktualnye problemy teorii i praktiki* [Criminal Procedural Law. Important Issues of Theory and Practice]. 3rd izd., pererab. i dop. Moscow, Yurayt Publ., 2016. 465 p.
10. Nekrasov S.V. *Yuridicheskaya sila dokazatelstv v ugolovnom sudoproizvodstve* [Juridical force of evidence in criminal procedure]. Moscow, Ekzamen Publ., 2004. 128 p.
11. Vasyaev A.A. *Priznanie dokazatelstv nedopustimymi v khode sudebnogo sledstviya v sude pervoy instantsii v rossiyskom ugolovnom protsesse* [Admission of evidence as incompetent in the course of a judicial investigation at first instance in the Russian criminal procedure]. Moscow, Volters Kluver Publ., 2010. 176 p.
12. Lazareva V.A., ed. *Ugolovnyy protsess* [Criminal process]. Moscow, YuSTITsIYa Publ., 2017. 654 p.
13. Lebedev A. Notary officers at the defense of the rights for Internet: securing of evidence by notary officers. *Peterburgskiy Notarius*, 2017, no. 2, pp. 3–4.
14. Shidlovskaya Yu.V. Certain issues related to the procedure of examination of an information resource. *Pravovye problemy ukrepleniya rossiyskoy gosudarstvennosti: sbornik statey*. Tomsk, Tom-kiy un-t Publ., 2012, pp. 137–139.
15. Sheyfer S.A. *Sledstvennye deystviya. Osnovaniya, protsessualnyy poryadok i dokazatelstvennoe znachenie* [Investigative actions. Grounds, a remedial order and probative value]. Samara, Samarskiy universitet Publ., 2004. 228 p.
16. Rossinskiy S.B. *Sledstvennye deystviya* [Investigative actions]. Moscow, Norma Publ., 2018. 240 p.
17. Olinder N.V. Typical ways of commission of crimes related to the using electronic payment means and systems. *Ekspert-kriminalist*, 2014, no. 1, pp. 13–15.
18. Bagmet A.M., ed. *Metodicheskie rekomendatsii po rassledovaniyu prestupleniy protiv polovoy neprikosnovennosti nesovershennoletnikh, sovershennykh posredstvom globalnoy seti "Internet"* [Methodological recommendations for investigation of crimes against the sexual inviolability of minors committed through the global Internet network]. Moscow, Akademiya Sledstvennogo komiteta Rossiyskoy Federatsii Publ., 2016. 73 p.
19. Stelmakh V.Yu. Obtaining Information about Connections between Subscribers and/or Subscriber Devices. *Lex Russica*, 2017, no. 3, pp. 141–153.
20. Gontar S.N., Uvarov N.A. The development of the constitutional right of individuals to privacy of the person in the field of criminal justice in modern history. *Vestnik Universiteta*, 2014, no. 13, pp. 290–292.
21. Aberkhaev E.R. The right on inviolability of privacy: the juridical characteristic and realization problems. *Aktualnye problemy ekonomiki i prava*, 2008, no. 1, pp. 90–94.

CONCERNING THE ISSUE OF PROCEDURAL IMPLEMENTATION OF THE EVIDENTIARY INFORMATION ACQUIRED FROM THE INTERNET SOURCES

S.V. Yunoshev, PhD (Law), Associate Professor, Head of Chair "Criminal Law and Procedure"
S.V. Kondratyuk, lecturer of Chair "Criminal Law and Procedure"
Togliatti State University, Togliatti (Russia)

Keywords: criminal procedure; evidential significance; investigative activities; survey of the information objects of the Internet network and communication network channels.

Abstract: This paper considers the significant issue of a criminal procedure – the attachment of the evidential significance of the information acquired from the information resources. The authors show that the current national criminal procedure legislation does not regulate special aspects of the introduction of such information to the evidentiary base. The thesis is substantiated that the lack of appropriate procedural regulation adversely affects the legality of proof when investigating and considering criminal cases, the reliability, and credibility of the acquired evidence. Whereby, it is stated that the needs of the law enforcement practice insistently require the filling of the current legislative gap as the other creates the risk of admission of the acquired evidence as incompetent and, as a consequence, the termination of a criminal prosecution or the entry of a judgment of acquittal. The authors draw attention that the similar procedures are known already and work successfully in other areas of Russian law, for example, in respect to the perpetuation of evidence by the notary officers. In this connection, the authors substantiate the suggestions about the introduction of additions to the Russian Federation Code of Criminal Procedure aimed at the introduction of a new type of survey, more specifically, a survey of the information objects of the Internet network and communication network channels. The authors substantiate as well the key distinctions of the proposed investigative activities from a standard survey of items and documents, which are mainly in the content of a protocol of inspection of the information resources, and consider the problem of provision of personal information about a network user by an organization rendering the Internet access services to an investigator (interviewer). Based on the analysis of current investigation practice, the conclusion is made about its contradiction to the constitutional guarantees for personal privacy established by the article 23 of the Russian Federation Constitution. Reasoning from this fact, the authors suggest protecting by law the possibility of requesting such information only on the basis of a judicial decision obtained under the procedure of the article 165 of the Russian Federation Code of Criminal Procedure.