УДК 343.1
doi: 10.18323/2220-7457-2023-3-13-19

Изъятие цифровых следов из сети Интернет и использование их в доказывании: уголовно-процессуальные аспекты

Гамбарова Евгения Александровна, магистр юриспруденции, магистр психологии,
аспирант, старший преподаватель кафедры «Уголовное право и процесс»
Тольяттинский государственный университет, Тольятти (Россия)

E-mail: **egambarova@yandex.ru** ORCID: https://orcid.org/0000-0002-9984-2819

Аннотация: В настоящее время увеличивается количество информации, которую пользователи сети Интернет размещают в ней и которой обмениваются друг с другом. Эта информация при определенных условиях может стать криминалистически значимой и в дальнейшем использоваться в качестве доказательств. Вопрос изъятия и процессуальной фиксации такой информации не регулируется действующим законодательством, что затрудняет использование этой информации в качестве доказательств. Цель исследования – выделить специфические признаки цифровой информации, особенности процесса доказывания с использованием цифровой информации и цифровых следов в рамках действующего уголовно-процессуального законодательства. Информация, полученная из социальных сетей, рассматривается автором в контексте цифровых следов и цифровых доказательств в уголовном процессе. Систематизированы признаки цифровых (электронных) доказательств. Проведен анализ положений ст. 74 Уголовно-процессуального кодекса Российской Федерации, а также современных научных подходов к пониманию системы и формы доказательств в уголовном процессе. Изучив правоприменительную практику, автор пришел к выводу, что существующая правовая регламентация использования цифровых (электронных) доказательств в уголовном процессе недостаточно эффективна. Анализ законодательства и правоприменительной практики в части использования цифровых следов в доказывании позволил сформулировать несколько предложений по совершенствованию норм уголовно-процессуального законодательства Российской Федерации. В частности, предложено закрепить в Уголовно-процессуальном кодексе РФ определение «цифровой документ», расширить перечень следственных действий и выделить отдельное следственное действие, направленное на обнаружение цифровых следов и фиксацию цифровой информации.

Ключевые слова: изъятие цифровых следов; ст. 74 УПК РФ; уголовный процесс; электронные доказательства; цифровые доказательства; социальные сети; собирание доказательств.

Для цитирования: Гамбарова Е.А. Изъятие цифровых следов из сети Интернет и использование их в доказывании: уголовно-процессуальные аспекты // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2023. № 3. С. 13–19. DOI: 10.18323/2220-7457-2023-3-13-19.

ВВЕДЕНИЕ

Развитие интернет-технологий дало толчок к преобразованиям во всех сферах жизни общества, в том числе в уголовном судопроизводстве. Результативность и эффективность расследования преступлений сегодня зависит не только от того, насколько участники уголовного процесса умеют пользоваться современными технологиями, но и – в большей степени – от того, насколько технологические новеллы восприняты законодателем и включены в уголовно-процессуальные нормы, насколько положения Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) отвечают требованиям времени, научно-техническому прогрессу, в том числе в части получения, сохранения, передачи и использования информации в целях доказывания по уголовному делу.

Вопросы обращения с информацией приобретают еще большее значение в контексте современного информационного общества. Информация – один из наиболее важных элементов общественной жизни и государственного управления, а также уголовного судопроизводства, основу которого составляет процесс собирания, проверки и оценки юридически значимых сведений (доказательств).

Теория уголовного процесса исходит из того, что любое событие, явление, деяние не проходит бесследно, оно всегда оставляет следы на материальном или идеальном носителе. В свою очередь, такие следы рассматриваются в качестве источников доказательств. При осуществлении уголовно-процессуальной деятельности орган расследования или суд получает с идеальных следов личные доказательства, с материальных следов – вещественные доказательства. Появление в начале XXI в. в уголовном процессе нового, неизвестного ранее виртуального следа и цифрового источника информации обозначило новую проблему: является ли цифровой след самостоятельным и уникальным, либо его стоит рассматривать в разрезе материального или идеального?

В первую очередь обозначенная проблема связана с получением органом расследования информации из социальных сетей, широко распространенных в настоящее время. Страница пользователя в социальной сети представляет собой хранилище данных о личности, и в определенной ситуации при производстве расследования по уголовному делу хранящаяся на ней информация может стать криминалистически значимой и послужить основой для формирования уголовно-процессуальных доказательств [1]. Чтобы информация стала

доказательством, нужно соблюсти ряд процессуальных требований, в частности правильно получить (собрать) информацию и преобразовать ее в доказательство, однако из-за специфических свойств виртуальных следов и цифровых доказательств этот процесс сопровождается пробелами, которые следует устранить посредством разработки и принятия специальных норм, регламентирующих порядок собирания, проверки и оценки цифровых доказательств.

Несмотря на стремительное развитие социальных сетей, проблема использования информации из них для доказывания по уголовным делам не была должным образом изучена и проанализирована ни в отечественной, ни в мировой науке. Имеется лишь ряд работ, посвященных смежным научным проблемам. Интересной представляется работа [2], в которой рассматриваются вопросы использования данных из социальных сетей в процессе доказывания по уголовным делам. Авторы дают обзор видов доказательств, полученных с помощью социальных сетей, а также наиболее распространенных средств, которые позволяют извлекать и анализировать эти доказательства.

Отдельного внимания заслуживает работа, посвященная доказыванию в условиях цифровизации общества[1], в которой отмечается, что эпоха цифровизации предъявляет новые требования к доказыванию. С одной стороны, использование цифровых технологий позволяет обеспечить высокую надежность и достоверность доказательств, так как они могут быть представлены в виде электронных документов, аудио- и видеозаписей, которые можно проверить на наличие подделок. С другой – цифровизация создает новые возможности для подделки и искажения доказательств, поэтому необходимо разрабатывать специальные методы и инструменты для их проверки и анализа. Автор считает, что в эпоху цифровизации важно развивать новые стандарты и методологии доказывания, которые бы учитывали особенности цифровых технологий и обеспечивали надежность и достоверность доказательств. Автор [3] одним из первых начал говорить о виртуальных следах и ввел в оборот понятие «виртуальный след». Он выделил особый механизм следообразования в кибернетическом пространстве, рассмотрел особенности электронно-цифрового отображения взаимодействующих объектов в искусственной среде, сформированной на основе компьютерных систем, раскрыл принципиальные особенности механизма следообразования в компьютерных системах, рассмотрел основные криминалистические свойства возникающих следов.

Цифровые технологии привносят как позитивные, так и негативные аспекты в процесс доказывания. Использование цифровых средств для сбора, хранения и представления доказательств может существенно упростить и ускорить процесс доказывания. В то же время возникает необходимость сохранения целостности и подлинности доказательств, полученных из сети Интернет, так как подобная информация может быть легко изменена [4; 5]. На основании анализа литературы можно прийти к выводу о необходимости разработки таких специальных методов и инструментов для проверки и аутентификации цифровых доказательств, которые бы обеспечивали их достоверность. В работах [6; 7] говорится о недостаточной регламентации использования доказательств, полученных из цифровых ресурсов.

Цель исследования – выделить специфические признаки цифровой информации и особенности процесса доказывания с использованием цифрового следа в рамках действующего уголовно-процессуального законодательства.

МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ

Исследование проходило в три этапа.

1. На основании анализа литературы было установлено, какими специфическими признаками обладает цифровой след, какие специфические свойства имеют цифровые доказательства.

2. На втором этапе стояла задача определить, какие пробелы существуют в уголовно-процессуальном законодательстве в части изъятия и фиксации цифровых следов и закрепления в качестве доказательств, а также проанализировать практику и действующее уголовно-процессуальное законодательство в части правовой регламентации порядка собирания информации с цифровых источников. Было проведено анкетирование практических сотрудников с целью определения границ исследования и понимания существующих проблем использования информации из сети Интернет в доказывании. На этом этапе изучалась следственная и судебная практика.

3. На основе полученной информации и проведенного исследования были разработаны предложения по совершенствованию уголовно-процессуального механизма работы с виртуальными следами, который обеспечивает сбор информации с цифровых источников, ее проверку и оценку.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

О необходимости включения понятия «цифровое доказательство» в уголовный процесс

В условиях перехода к информационному обществу и бурной цифровизации уголовного процесса остается дискуссионным вопрос о природе цифровых доказательств, о корректности использования этого термина как такового. В научном сообществе на протяжении длительного времени ведется дискуссия о необходимости включения понятия «цифровое доказательство» в уголовный процесс. Следует признать, что в некоторых иностранных государствах уже давно признали существование электронных доказательств и выработали методику работы с цифровыми следами. В 2013 г. Генеральный секретарь ООН говорил о необходимости применения правоохранительными органами новых методов работы при расследовании преступлений [8]. В США для этой цели существуют готовые технические решения, в частности, некоторые частные компании предоставляют услуги по фиксации цифровых следов. С целью применения правоохранительными органами новых методов работы с цифровыми доказательствами предлагается дополнить ст. 74 УПК РФ понятием «цифровое доказательство» [9].

[1] *Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. № 4. С. 46–50. EDN: XXXCNP.*

Признаки цифровых следов как специфической формы преобразования информации

Предложение дополнить ст. 74 УПК РФ понятием «цифровое доказательство» представляется целесообразным, так как цифровые следы, как специфическая форма преобразования компьютерной информации, обладают следующими признаками:

1) отражают событие преступления в информационном поле;

2) являются материальными по своей природе;

3) неочевидны по содержанию и могут содержать в себе скрытую от восприятия информацию, которая может быть обнаружена только с помощью специальных знаний и средств;

4) служат носителями свойств, присущих компьютерной информации;

5) обладают способностью к дублированию;

6) изменчивы (в них легко можно внести изменения, при этом без использования специальных знаний и средств трудно определить, были ли внесены изменения, когда и кем).

Отличие цифрового доказательства от доказательств, источниками которых является материальный или идеальный носитель

Если цифровое доказательство по своему содержанию полностью соответствует ч. 1 ст. 74 УПК РФ, значит, оно ничем не отличается от доказательств, источниками которых является материальный или идеальный носитель.

Учитывая, что цифровые доказательства специфичны по своей форме (ч. 2, 3 ст. 74 УПК РФ), целесообразно предложить отдельный вид доказательства в форме цифрового документа. При таком подходе речь идет не о самостоятельном цифровом доказательстве, а об отдельном виде уголовно-процессуального доказательства – цифровом документе.

Мы исходим из того, что цифровая информация должна быть введена в уголовный процесс в качестве отдельного вида доказательства, для чего следует дополнить ч. 2 ст. 74 УПК РФ пунктом «цифровые документы». Основанием для выделения цифрового документа является его уникальность и специфичность, проявляющаяся как в источниках данного вида доказательства, так и в его следообразовании. Если доказательство в виде «иного документа» всегда имеет материальную природу, так как непосредственно связано с материальным следом и объектом (источником), на котором он располагается, то цифровой след принципиально отличен.

Классификация следов в уголовном процессе и специфические свойства цифрового следа

Во-первых, источник цифрового документа не связан с определенным материальным объектом. Во-вторых, виртуальные следы обладают способностью сохранять свою структуру и содержание без изменений. Данное свойство особенно важно для обеспечения целостности цифровой информации при подтверждении экспертиз. В-третьих, цифровые следы могут быть уникально идентифицированы и связаны с конкретными событиями, лицами или устройствами. В-четвертых, цифровые следы обладают свойством персистентности, т. е. сохраняются в цифровой среде в течение длительного времени и могут быть восстановлены и воспроизведены после удаления и изменения.

Не является цифровой след идентичным и идеальным следам, под которыми принято понимать образы в сознании человека, возникающие в результате его когнитивных процессов. Принципиальные различия носителей материальных (материальный объект), идеальных (сознание человека) и виртуальных (цифровой ресурс) следов обуславливают необходимость выделения трех видов доказательств – вещественных, личных и цифровых, и трех процедур, обеспечивающих их собирание (рис. 1).

Если по первым двум видам доказательств законодатель разработал соответствующие процедуры, то работа

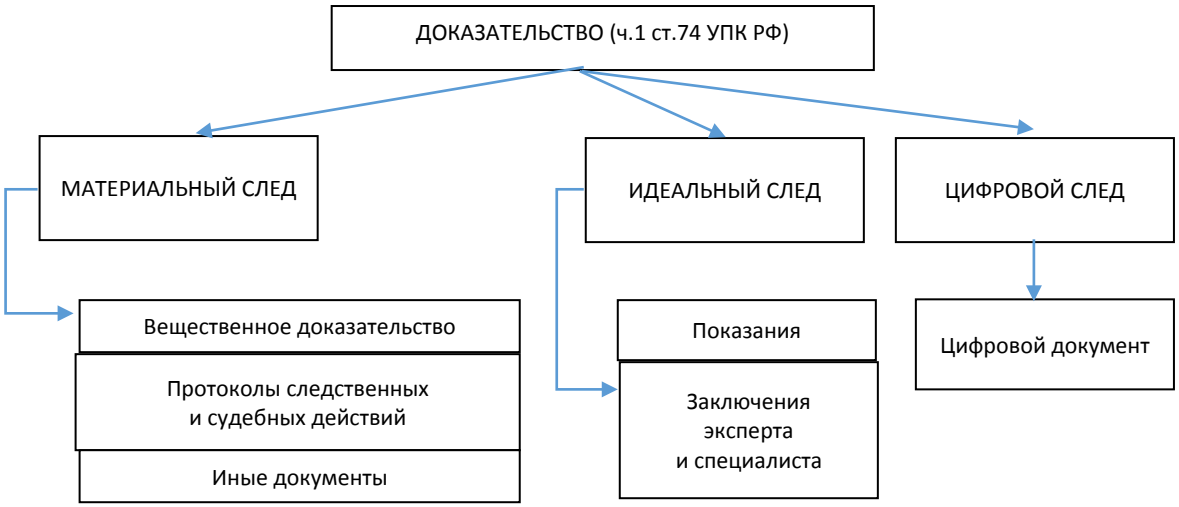

Рис. 1. *Классификация следов в уголовном процессе*

с цифровыми следами пока остается вне правового регулирования, и правоприменитель здесь вынужден действовать самостоятельно. Как это происходит в практической деятельности органов расследования, рассмотрим на примере получения информации из социальных сетей.

Социальные сети являются площадкой, на которой пользователи размещают большое количество информации (в том числе и криминалистически значимой), тем самым оставляя цифровые следы, которые при правильном их изъятии и оформлении смогут в дальнейшем выступать доказательствами по делу.

Социальные сети как источник информации

С помощью социальных сетей может быть осуществлен:

1) сбор информации о подозреваемых, свидетелях и потерпевших. Цифровые ресурсы, такие как страница пользователя в социальной сети, представляют собой хранилище данных о личности. В определенной ситуации эта информация может стать криминалистически значимой и послужить основой для формирования уголовно-процессуальных доказательств. С помощью цифровых ресурсов может быть осуществлен сбор информации о личности [10], установление связей, анализ поведения и составление психологического портрета;

2) установление связей между лицами, имеющими отношение к исследуемому событию;

3) анализ поведения участников уголовного процесса. Эта информация может быть полезной как для определения тактики следственных действий, так и для выбора мер пресечения.

Важной особенностью при работе с информацией из социальных сетей является то, что страница в социальной сети содержит большое количество информации за разные года, и следователь на этапе осмотра страницы может не знать, какие данные ему могут в дальнейшем понадобиться. На практике чаще всего изымается либо переписка, либо копируются (методом скриншота) какие-либо фотографии. Далее эта информация (копии переписки, фото) переносится в протокол соответствующего следственного действия. Предметом осмотра страницы в социальной сети является криминалистически значимая информация.

Преобразование информации из социальных сетей в уголовно-процессуальные доказательства

Как правило, следователи производят осмотр страницы в сети Интернет посредством такого следственного действия, как осмотр предметов, при этом в протоколе указывают, что объектом осмотра выступает компьютер, несмотря на то что фиксированные данные находятся не в памяти компьютера [11]. Очень подробно проблемы собирания цифровых следов преступлений из социальных сетей рассмотрены в [12]. Расположение материальных носителей может быть неизвестно или находиться вне юрисдикции РФ. Помимо данного следственного действия, могут использоваться и другие формы фиксации доказательственной информации. Достаточно обстоятельно этот вопрос рассмотрен авторами [13], которые на основе анализа судебной практики выделили следующие способы оформления информации, содержащейся в сети Интернет:

1) составление протокола осмотра с приложением к нему электронных носителей информации, полученных или скопированных с других электронных носителей информации в ходе производства следственного действия;

2) составление протокола осмотра с приложением к нему материалов фото- и видеосъемки. Например, для фиксации информации с интернет-сайта следователем производилась фотосъемка страницы сайта;

3) составление протоколов допроса участников уголовного судопроизводства, которые могут подтвердить или опровергнуть наличие информации в сети Интернет;

4) составление протокола осмотра и выемки предметов, которые использовались для размещения информации в сети Интернет;

5) приобщение к материалам дела справок, выписок, заверенных копий документов, полученных в ходе официальных запросов, имеющихся в материалах уголовного дела. Например, истребованная в сотовых компаниях информация о соединениях абонентов и абонентских устройств с указанием месторасположения базовых станций, истребования информации у интернет-провайдеров, истребования информации у компаний, владеющих социальными сетями и мессенджерами. Компании, которые находятся вне юрисдикции РФ, информацию могут не предоставить;

6) назначение соответствующего вида экспертизы по изъятым электронным носителям.

Опрос 102 сотрудников правоохранительных органов (следователей и дознавателей МВД РФ и следователей следственного комитета РФ), проведенный в рамках нашего исследования, подтвердил, что процессуальными средствами извлечения цифровой информации являются осмотр предметов и документов, судебная экспертиза. Приобщение к материалам уголовного дела осуществляется постановлением протокола осмотра предмета (персонального компьютера, ноутбука, планшета, смартфона и т. д.) или протоколом осмотра вебсайта (страницы в сети Интернет, страницы пользователя в социальной сети). При возможности к делу приобщается носитель (по аналогии с процессуальными средствами извлечения криминалистически значимых сведений с электронных носителей). Проблема заключается в том, что у следователя может не быть доступа к физическому носителю (он может находиться вне юрисдикции РФ). Стоит отметить, что в настоящее время нет единой практики приобщения цифровой информации к материалам уголовного дела.

Важно не только пресечь возможность изменения и удаления информации (что сегодня легко осуществляется через удаленный доступ), но и зафиксировать информацию в том виде, в котором она присутствовала на момент осмотра, с сохранением всех оставленных на ней электронных следов.

Следует подчеркнуть важный момент. Если осмотр осуществляется только следователем, а результаты осмотра фиксируются в виде распечатанных скриншотов (которые позже приобщаются к протоколу осмотра страницы в социальной сети), через какое-то время следователь может понять, что он, например, не проанализировал активность пользователя в определенных группах, не составил его психологический профиль (с целью выбора тактики проведения следственного

действия), однако получение такой дополнительной информации может быть уже невозможным.

Осмотр информации из социальных сетей может быть проведен с любого устройства, которое предназначено для работы в сети Интернет (ПК, ноутбук, планшет, смартфон), так как большей частью информация имеет возможность удаленного доступа. Может использоваться как устройство подозреваемого, так и устройство следователя. С момента осмотра необходимо пресечь возможность изменения данных, что весьма затруднительно, так как недостаточно просто ограничить доступ подозреваемому к указанным ресурсам. Если у другого заинтересованного лица есть пароли и логины от социальных сетей и мессенджеров подозреваемого, облачных хранилищ и т. д., информация может быть удалена им дистанционно из другой точки мира.

Во избежание потери данных, а также облегчения работы следователя необходимо составить процессуальную регламентацию и криминалистические рекомендации по работе с информацией из социальных сетей. Так как информацию, которую необходимо зафиксировать из социальной сети, невозможно зафиксировать только скриншотами, необходима дополнительная информация о точках доступа и история изменения (удаления) информации. Цифровые следы в целом содержат много информации, которую не видно невооруженным взглядом. Цифровые следы в дальнейшем могут быть использованы в качестве цифровых доказательств.

Цифровые доказательства обладают специфичными признаками, которые требуют специфического подхода к работе с ними и фиксации их в качестве доказательств. Часть авторов сегодня склоняется к тому, что при работе с электронными доказательствами необходимо утвердить форму электронных протоколов фиксации информации, содержащейся в таких доказательствах. Электронные протоколы имеют возможность фиксации материалов без искажения и упущения, которое происходит при фиксации в протоколе в письменном виде. В гражданском процессе применяются программы для удостоверения цифровых доказательств, т. е. технические решения существуют, но процессуальной возможности их использования нет.

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

В настоящее время нет единого эффективного уголовно-процессуального механизма использования информации из сети Интернет в доказывании. Некорректная с процессуальной точки зрения фиксация информации из сети Интернет может привести к потере самого доказательства. Требуется регламентация правил собирания, проверки и оценки электронных (цифровых) доказательств (к которым в том числе относится информация из социальных сетей). При этом важно работать не только над процессуальной регламентацией обращения с цифровыми доказательствами, но и над методологическими аспектами их использования. Представляется целесообразным продолжать исследование вопроса использования информации из сети Интернет в процессе доказывания.

Проведенное исследование позволяет сделать вывод о целесообразности включения термина «цифровой документ» в уголовный процесс, введение нового следственного действия по обнаружению цифровых следов и фиксации цифровой информации. Игнорирование необходимости специфического правового регламентирования работы с цифровыми доказательствами в уголовном процессе может приводить к потере доказательств.

Действующий уголовно-процессуальный закон предусматривает фиксацию уголовно-процессуальных доказательств в письменном виде в соответствии с ч. 2 ст. 74 УПК РФ. Данная норма является несовершенной и не позволяет сохранять цифровую доказательственную информацию исключительно в электронном виде и использовать ее в доказывании [15] именно в электронном виде. Сложность перевода цифрового доказательства в письменную форму заключается в том, что трудно перенести в письменный вид весь объем информации, который содержится даже на одной странице веб-сайта.

Признаки и свойства цифровых доказательств:

1) доступность для восприятия человеком только при использовании ЭВМ. Информация на бумажном носителе может быть непосредственно прочитана, однако информация на электронном носителе требует расшифровки, преобразования в форму, пригодную для прочтения человеком;

2) пригодность для передачи по информационно-телекоммуникационным сетям. Согласно п. 4 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационной сетью является «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»;

3) пригодность для обработки в информационных системах. В соответствии с п. 3 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» под информационной системой понимается «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств»;

4) труднодоступность первоисточника. Первоисточник хранится на устройствах, которые могут находиться вне юрисдикции РФ. Соответственно, не всегда возможно получение данных из первоисточника;

5) возможность удаления и изменения дистанционно. Информация может быть дистанционно изменена или удалена из любой точки мира в любой момент любым пользователем, имеющим к ней доступ.

Еще одна проблема, возникающая при использовании электронных доказательств в уголовном судопроизводстве, связана с существенной разницей между бумажной и электронной формой доказательств [16], что обусловлено природой цифровых следов. В классической трасологии выделяются материальные и идеальные следы, и для них существуют определенные формы, которые учитывает ст. 74 УПК РФ. Для цифровых следов в настоящее время специфической формы нет, хотя специфические свойства есть: возможность неограниченного копирования без нарушения целостности первоисточника информации; несложная процедура уничтожения как первичной информации, так и ее копий [17].

Работа с цифровыми доказательствами представляется более технически сложным процессом в связи с тем, что это, пожалуй, единственный тип доказательств, в которые могут быть внесены изменения или

которые могут быть удалены дистанционно из любой точки мира. Цифровые доказательства – это всегда производные доказательства, они не могут быть первоначальными, в отличие от вещественных и личных доказательств. В условиях цифровизации общества уголовный процесс также попал под влияние информационно-технического прогресса, что обусловило необходимость процессуального и методологического регулирования использования цифровых доказательств.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

1. Введено понятие нового вида доказательства «цифровой документ» и раскрыто его содержание.

2. Предложена новая классификация доказательств по их следообразованию, выделены вещественные, личные и цифровые доказательства с указанием особенностей каждого вида.

3. Рассмотрена возможность использования в уголовном процессе информации из цифровых ресурсов, в частности сбор криминалистически значимой информации, выбор тактики следственных действий в процессе доказывания, использование информации из цифровых ресурсов в качестве доказательств.

СПИСОК ЛИТЕРАТУРЫ

1. Карепанов Н.В. Некоторые вопросы выявления и исследования преступлений // Российское право: образование, практика, наука. 2019. № 3. С. 49–60. DOI: 10.34076/2410-2709-2019-3-49-60.
2. Seigfried-Spellar K.C., Leshney S.C. Chapter 4 – The intersection between social media, crime, and digital forensics: Who Dun It? // Digital Forensics Threatscape and Best Practices. Threatscape and Best Practices. 2016. P. 59–67. DOI: 10.1016/B978-0-12-804526-8.00004-6.
3. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: ВГУ, 2001. 255 с.
4. Жарова А.К. Особенности процесса правовой идентификации человека в Интернете // Информационное право. 2016. № 3. С. 30–35. EDN: WTQNHH.
5. Колычева А.Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет // Вестник Удмуртского университета. Серия экономика и право. 2017. Т. 27. № 2. С. 109–113. EDN: YLFUDL.
6. Количенко А.А. Электронные носители информации как источник получения электронных доказательств в уголовном процессе // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 1. С. 114–121. EDN: MHOATZ.
7. Девяткин Г.С., Луценко П.А. Переписка в мессенджерах и социальных сетях как доказательство по уголовному делу // Государственная служба и кадры. 2021. № 2. С. 159–161. EDN: VYNNKR.
8. Высокотехнологичный уголовный процесс / под ред. С.В. Зуева, Л.Н. Масленниковой. М.: Юрлитинформ, 2023. 216 с.
9. Балашова А.А. К вопросу о понятии «электронное доказательство» // Закон и право. 2018. № 6. С. 120–122. DOI: 10.24411/2073-3313-2018-10031.
10. Призенко А.Д., Шевелёва К.В. Интернет-профиль как источник информации личности допрашиваемого // Учёные записки Казанского юридического института МВД России. 2023. Т. 8. № 1. С. 87–91. EDN: DEUZHC.
11. Карлов А.Л. Использование в доказывании по уголовным делам сведений, составляющих тайну связи, расположенных в сети Интернет // Вестник Сибирского юридического института ФСКН России. 2015. № 2. С. 142–146. EDN: TXICJX.
12. Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3. С. 106–123. EDN: YKCUUH.
13. Губарева Е.К., Калентьева Т.А. Особенности фиксации информации содержащейся в сети интернет // Вестник Волжского университета имени В.Н. Татищева. 2019. Т. 1. № 2. С. 161–168. EDN: ZHCFAD.
14. Рамалданов Х.Х. Проблем использования и хранения цифровых доказательств в доказывании в уголовном процессе // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 2. С. 105–111. EDN: ZCISQR.
15. Иванов В.Ю. К вопросу о классификации электронно-цифровых следов // Национальная безопасность/Nota bene. 2020. № 3. С. 64–71. DOI: 10.7256/2454-0668.2020.3.33308.
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. DOI: 10.12737/jflcl.2019.4.4.
17. Воронин М.И. Особенности оценки электронных (цифровых) доказательств // Актуальные проблемы российского права. 2021. Т. 16. № 8. С. 118–128. DOI: 10.17803/1994-1471.2021.129.8.118-128.

REFERENCES

1. Karepanov N.V. Some issues of detection and investigation of traces of crimes. *Rossiyskoe pravo: obrazovanie, praktika, nauka*, 2019, no. 3, pp. 49–60. DOI: 10.34076/2410-2709-2019-3-49-60.
2. Seigfried-Spellar K.C., Leshney S.C. Chapter 4 – The intersection between social media, crime, and digital forensics: Who Dun It? *Digital Forensics Threatscape and Best Practices. Threatscape and Best Practices*, 2016, pp. 59–67. DOI: 10.1016/B978-0-12-804526-8.00004-6.
3. Meshcheryakov V.A. *Prestupleniya v sfere kompyuternoy informatsii: pravovoy i kriminalisticheskiy analiz* [Cyber crimes: legal and criminalistics analysis]. Voronezh, VGU Publ., 2001. 255 p.
4. Zharova A.K. Special aspects of legal identification of a person in the internet. *Informatsionnoe pravo*, 2016, no. 3, pp. 30–35. EDN: WTQNHH.
5. Kolycheva A.N. Some aspects of fixing of the evidentiary information stored on the resources of the Internet. *Vestnik Udmurtskogo universiteta. Seriya ekonomika i pravo*, 2017, vol. 27, no. 2, pp. 109–113. EDN: YLFUDL.

6. Kolichenko A.A. Electronic media as a source of obtaining electronic evidence in criminal proceedings. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*, 2022, vol. 13, no. 1, pp. 114–121. EDN: MHOATZ.
7. Devyatkin G.S., Lutsenko P.A. Correspondence in messengers and social networks as evidence in a criminal case. *Gosudarstvennaya sluzhba i kadry*, 2021, no. 2, pp. 159–161. EDN: VYNNKR.
8. Zuev S.C., Maslennikova L.N., eds. *Vysokotekhnologichnyy ugolovnyy protsess* [High-technology criminal procedure]. Moscow, Yurlitinform Publ., 2023. 216 p.
9. Balashova A.A. On the question of concept "electronic evidence". *Zakon i pravo*, 2018, no. 6, pp. 120–122. DOI: 10.24411/2073-3313-2018-10031.
10. Prizenko A.D., Sheveleva K.V. Personal web page as a source of information about an interrogate. *Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii*, 2023, vol. 8, no. 1, pp. 87–91. EDN: DEUZHC.
11. Karlov A.L. The usage of the secret communication data located on the internet in proving criminal cases. *Vestnik Sibirskogo yuridicheskogo instituta FSKN Rossii*, 2015, no. 2, pp. 142–146. EDN: TXICJX.
12. Rossinskaya E.R., Saakov T.A. The problems of collecting digital footprints of crimes in social networks and messengers. *Kriminalistika: vchera, segodnya, zavtra*, 2020, no. 3, pp. 106–123. EDN: YKCUUH.
13. Gubareva E.K., Kalenteva T.A. Features of recording information contained on the internet. *Vestnik Volzhskogo universiteta imeni V.N. Tatishcheva*, 2019, vol. 1, no. 2, pp. 161–168. EDN: ZHCFAD.
14. Ramaldanov Kh.Kh. Using and storing digital evidence in proving in criminal proceedings. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*, 2023, vol. 14, no. 2, pp. 105–111. EDN: ZCISQR.
15. Ivanov V.Yu. To the question on classification of digital footprint. *Natsionalnaya bezopasnost/Nota bene*, 2020, no. 3, pp. 64–71. DOI: 10.7256/2454-0668.2020.3.33308.
16. Zaytsev O.A. Features of the use of electronic information as criminal evidence: a comparative-legal analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatelstva i sravnitelnogo pravovedeniya*, 2019, no. 4, pp. 42–57. DOI: 10.12737/jflcl.2019.4.4.
17. Voronin M.I. Characteristics of electronic (digital) evidence assessment. *Aktualnye problemy rossiyskogo prava*, 2021, vol. 16, no. 8, pp. 118–128. DOI: 10.17803/1994-1471.2021.129.8.118-128.

Seizure of digital footprints from the Internet and their use in evidence: criminal procedural aspects

Evgeniya A. Gambarova, Master of Law, Master of Psychology,
postgraduate student, senior lecturer of Chair "Criminal Law and Procedure"
Togliatti State University, Togliatti (Russia)

E-mail: **egambarova@yandex.ru** ORCID: https://orcid.org/0000-0002-9984-2819

Abstract: Currently, the amount of information that Internet users post on it and exchange with each other is increasing. Under certain conditions, this information, can become forensically significant and can be used as evidence in the future. The issue of seizure and procedural recording of such information is not regulated by current legislation, which makes it difficult to use this information as evidence. The purpose of the study is to identify specific features of digital information, special aspects of the process of proof using digital information and digital footprints within the framework of the current criminal procedure legislation. The author considers the information obtained from social networks in the context of digital footprints and digital evidence in criminal procedure. The signs of digital (electronic) evidence have been systematized. The author carried out an analysis of the provisions of Art. 74 of the Criminal Procedure Code of the Russian Federation, as well as of modern scientific approaches to understanding the system and form of evidence in criminal procedure. Having studied law enforcement practice, the author concluded that the existing legal regulation of the use of digital (electronic) evidence in criminal procedure is not effective enough. The analysis of legislation and law enforcement practice regarding the use of digital footprints in evidence allowed formulating several proposals to improve the norms of criminal procedure legislation of the Russian Federation. In particular, the author proposed to enshrine the definition of digital document in the Criminal Procedure Code of the Russian Federation, expand the list of investigative actions, and specify a separate investigative action aimed at detecting digital footprints and recording digital information.

Keywords: seizure of digital footprints; Article 74 of the RF Criminal Procedure Code; criminal procedure; electronic evidence; digital evidence; social networks; collection of evidence.

For citation: Gambarova E.A. Seizure of digital footprints from the Internet and their use in evidence: criminal procedural aspects. *Vektor nauki Tolyattinskogo gosudarstvennogo universiteta. Seriya: Yuridicheskie nauki*, 2023, no. 3, pp. 13–19. DOI: 10.18323/2220-7457-2023-3-13-19.