УДК 343.13

КРИМИНАЛИСТИЧЕСКИЕ ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ, ФИКСАЦИИ, ИЗЪЯТИЯ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ

Маевский С.С., Зайцева А.Н.

Брянский государственный университет имени академика И.Г. Петровского, г. Брянск

Статья посвящена анализу электронных доказательств в уголовном процессе РФ. Рассматриваются правовые основы их использования, способы фиксации и особенности процессуального оформления. Освещаются требования к работе с электронными носителями, роль специалистов и судебная практика. Особое внимание уделено вопросам допустимости цифровых данных, их сохранности и интерпретации. Материал актуален для правоприменителей, сталкивающихся с расследованием киберпреступлений и применением современных технологий в уголовном судопроизводстве.

Ключевые слова: электронные доказательства, уголовный процесс, цифровые следы, криминалистика, УПК РФ, судебная практика, информационные технологии, материальные носители, оперативно-розыскные мероприятия.

DOI 10.22281/2542-1697-2025-04-02-162-169

Доказательствами в уголовном процессе РФ, согласно ст. 74 УПК РФ [1], являются сведения, позволяющие установить обстоятельства, подлежащие доказыванию. Информация о преступной деятельности фиксируется людьми (в процессе мысленной деятельности) или автоматически (с помощью алгоритмов программ) [13, с. 698].

Электронные доказательства могут быть представлены как электронные сообщения (данные, переданные через интернет, согласно ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3]) или электронные документы (документированные сведения в цифровом формате). Они признаются доказательствами в качестве вещественных (ст. 81 УПК РФ) или иных документов (ст. 84 УПК РФ).

Цель фиксации таких доказательств - закрепить факты, связанные с преступлением. В криминалистике ключевое значение имеет процесс выявления и сохранения компьютерных данных, включая методы их обработки и используемые средства.

Поговорим о фиксации доказательств, которые представлены в электронном виде [7, с. 18]:

1) доказательные компьютерные данные, содержащиеся в исходном произведении, перекодируются в понятную человеку форму, например, отображаются на экране (мониторе) компьютерного устройства или прослушиваются в виде фонограммы;

2) компьютерные данные изымаются с помощью визуального (материального) носителя и (или) копируются на другой визуальный (материальный) носитель, захват которого нецелесообразен или невозможен;

3) хранение компьютерных данных, являющихся доказательствами, сохраняется для многократного использования при получении доказательств, например, при проведении судебно-медицинских экспертиз, раскрытии в качестве доказательств при перекрёстном допросе;

4) благодаря сохранению зафиксированного «местонахождения» компьютерных данных можно накапливать их до необходимого уровня, то есть до тех пор, пока не будут проверены все факты, которые необходимо установить;

5) обеспечивается возможность отбора данных о преступном деянии, то есть не фиксируются все компьютерные данные, полученные работником следственной группы или судьей, а только те, которые имеют значение для выдачи доказательств (релевантные компьютерные данные). по уголовно-процессуальному закону Российской Федерации (допустимые компьютерные данные) и актуальны в контексте доказательств;

6) «запечатлевается не только сама доказательственная компьютерная информация, но и

информация о путях, способах её получения как необходимое условие признания ее допустимости по делу» [9, с. 47].

Электронные носители, имеющие значение для дальнейшего рассмотрения и разрешения уголовного дела, собираются при проведении следственных действий с привлечением специалиста. По требованию правообладателя изъятых электронных архивов или собственника информации о них специалист, участвующий в следственном действии, в присутствии понятых производит копирование данных из изъятых электронных носителей. Информация копируется на другие электронные носители, предоставленные законным владельцем захваченного (изъятого) электронного носителя или владельцем содержащейся на нем информации.

Обратимся к материалам судебной практики: Советский районный суд города Орска признал лицо виновным в совершении преступления, которое предусмотрено пунктом «г» части 4 статьи 228.1 Уголовного кодекса Российской Федерации со ссылкой на часть 3 статьи 30 Уголовного кодекса Российской Федерации [17]. Указанная уголовно-правовая норма предусматривает установление ответственности за совершение такого общественно опасного деяния, как покушение на сбыт наркотических и психотропных средств, совершённое в крупном размере. При этом виновное лицо подало апелляционную жалобу, суть которой сводилась к тому, что его мобильный телефон – электронный носитель информации, был изъят с нарушением части 3.1 статьи 183 Уголовно-процессуального кодекса России, которая устанавливает обязательное участие специалиста.

Вышестоящая судебная инстанция, рассмотрев апелляционную жалобу виновного в преступлении лица, пришла к выводу о том, что указанные им доводы являются необоснованными, поскольку часть 3.1 статьи 183 Уголовно-процессуального кодекса Российской Федерации устанавливает правило, согласно которому участие специалиста при изъятии электронных носителей информации, в том числе и мобильных телефонов, продиктовано таким понятием как «нуждаемость». Иными словами, если при осуществлении следственных действий не совершаются действия, которые требуют применения специальных навыков и познаний, участие специалиста является необязательным. Ситуации, в которых его участие необходимо (обязательно) сводится к тому, когда при изъятии электронного носителя возможно утратить или изменить информацию, которая имеет значение для рассмотрения и разрешения уголовного дела.

В процессе осуществления следственного действия на следователя ложится обязанность по копированию сведений, которые находятся на изымаемом электронном носителе. В дальнейшем ему следует отметить в протоколе шаги, которые были предприняты для копирования данных, способы их использования, шаги, а также полученные результаты. Кроме того, к нему должны быть приложены электронные носители данных, содержащие информацию из других носителей, и обнаруженные в процессе осуществления следственного действия. Указанные правила содержатся в статье 164.1 Уголовно-процессуального кодекса Российской Федерации.

Примером сказанного может быть ситуация, в которой сотрудники органов внутренних дел обследовали различные сооружения, участки местности и транспортных средств, и изъяли при этом электронные документы. В данном случае сотрудник обязан предпринять все меры, которые направлены, во-первых, на недопущение уничтожения изымаемой информации, и, во-вторых, на обеспечение возможности изготовления копии лицом, у которого изымаются электронные документы. Указанное правило содержится в пункте 11 Инструкции «О порядке проведения сотрудниками органов внутренних дел Российской Федерации гласного оперативно-розыскного мероприятия обследование помещений, зданий, сооружений, участков местности и транспортных средств» [5].

Эти требования распространяются и на оперативно-розыскное мероприятие «Получение компьютерной информации», правила проведения которого предусмотрены пунктом 15 статьи 6 Федерального закона «Об оперативно-розыскной деятельности» [2].

Средства защиты в соответствии с пунктом 7 приложения 1 Положения «О системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну» [4]:

1) защита информации от копирования, произведённого несанкционированным способом,

которая включает в себя также меры, направленные на защиту носителей электронной информации, и на предотвращение копирования программного обеспечения, которое устанавливается на компьютерном устройстве;

2) защита криптографической и стеганографической информации, которая осуществляется при хранении и передаче такой информации, а также включает средства, направленные на маскирование сведений;

3) прерывание функционирования программы, которая имеет своей целью нарушить установленные правила доступа, и к которой можно отнести также принудительное завершение работы и блокировку электронно-вычислительной машины;

4) удаление (стирание) информации, включая и остаточную;

5) установление сигнала тревоги, который возникает при осуществлении несанкционированного доступа, и который также может включать установление контроля за действиями пользователей;

6) выявление вредоносных программ, а также прекращение их негативного воздействия.

Отметим, «что чаще других в качестве вещественных доказательств рассматриваемого вида выступают электронные подписи и электронные ключи» [10, с. 78].

Таким образом, процесс формирования (возникновения) цифровых следов преступного посягательства – это довольно сложный, многоуровневый процесс, требующий специальных навыков и опыта от специалистов по преступности и информационной безопасности.

Уголовно-процессуальным кодексом Российской Федерации, а именно статьей 166 указанного нормативно-правового акта, предусмотрено, что обеспечение расследования (выемки, обыска) дополняется, в частности, электронными носителями, полученными или скопированными из других источников в ходе производства следственного действия.

В соответствии с положениями, закреплёнными в части 2 статьи 177 Уголовно-процессуального кодекса Российской Федерации, осуществление осмотра предметов, являющихся электронными носителями информации, производится в рамках того следственного действия, в ходе которого и они были выявлены.

В ходе осмотра таких носителей, в первую очередь, важно выявить те следы и признаки, которые могут стать в последующем объектами для исследования, проводимого экспертами. При этом необходимо соблюдать правила, которые направлены на обеспечение сохранения доказательственной силы электронных носителей информации.

Одним из важнейших условий наиболее эффективного изъятия электронных носителей – это участие в данном действии специалиста. В настоящее время оно носит рекомендательный характер.

В частности, отсутствие специалиста в момент изъятия электронных данных является нарушением положений, закреплённых статьёй 164.1 Уголовно-процессуального кодекса Российской Федерации. Это даёт возможность исключить из круга доказательств не только протокол, но и любую процессуальную документацию, который был составлен на основании его результатов.

Примером сказанного может выступить Приговор Индустриального районного суда города Барнаула [16], в котором судья признал протокол выемки текстовых сообщений с сайта в сети Интернет, был признан недопустимым доказательством вследствие того, что в соответствии с положениями вышеуказанной уголовно-процессуальной нормы к данному следственному действию не был привлечён специалист. Недопустимыми также были признаны протокол осмотра и непосредственно распечатка сообщений.

На первоначальной стадии, которую мы назвали ранее, выявляются электронные устройства (ноутбуки, компьютеры и иные электронные вычислительные машины), которые могут являться электронными носителями данных. Эксперты (специалисты) на обзорной стадии рекомендуют опасаться не подключённых розеток, поскольку перед тестированием электронные устройства могли быть выключены и спрятаны, а также устройства с беспроводным подключением, особенно Wi-Fi [11, с. 41].

На второй стадии, указанной нами, осмотру подлежит каждое устройство по отдельности.

Данные действия осуществляются для поиска и дальнейшего изъятия носителей информации, которые могут иметь значение для рассмотрения и разрешения уголовного дела.

При запуске компьютера информация, отображаемая на экране монитора, а также состояние индикаторов на мониторе и клавиатуре фиксируются путем фото- или видеозаписи, а также распознаётся соответствующее программное обеспечение. После нормального выключения компьютерного оборудования решается вопрос, изъятия связанного с ним хранилища (электронного носителя информации).

Отметим, что изъятие планшетов, ноутбуков и иных переносных устройств осуществляется полностью, а вот громоздкие электронно-вычислительные машины подлежат частичному изъятию – сетевые блоки, электронные накопители и так далее. Кроме того, может рекомендоваться изъятие информации, осуществляемое в лабораторных условиях специалистами.

Копирование с изъятых электронных носителей является частью процесса расследования, определённого следственного действия, к которому можно отнести обыск или выемку, а не самостоятельным процессом, процессуальным действием. В момент изъятия копирование из электронного носителя в другой может быть произведено только специалистом дополнительно к электронному носителю, находящемуся у законного владельца, либо по требованию владельца информации [8, с. 36].

После осуществления вышеуказанных манипуляции с мобильным телефоном или смартфоном во время проведения того или иного следственного действия, его следует правильно выключить – это действие обеспечит сохранение содержимого данных. В протоколе следственного действия должны быть указаны способ отключения мобильного телефона или смартфона, а также точные дата и время. Указанные устройства необходимо поместить в герметичный пакет, чтобы случайно не нажать на клавиатуру или кнопку включения во время дальнейшей транспортировки и хранения. «При транспортировке изъятого имущества должны соблюдаться меры, исключающие возможность повреждения» [6, с. 12].

Особый интерес для следователей представляет история посещения лицами, участвующими в преступных деяниях, определённых (конкретных) страниц накануне совершения преступления – во время его подготовки, а также последующего исполнения или даже в ходе расследования.

В момент получения, записи и фиксации цифровой информации необходимо установить природу её происхождения. Для этого необходимо проследить цепочку и (или) связи, возникающие от компьютера, на котором были обнаружены следы преступления, до компьютера, на котором физически работал обвиняемый. Большая часть таких коммуникаций происходит онлайн, которые состоят из множества локальных и глобальных сетей, принадлежащих различным организациям, агентствам и ведомствам, соединенных между собой множеством каналов связи [12, с. 101].

Структура информации, которая размещается в глобальной сети под наименованием Интернет, по форме в целом аналогична структуре цифровых доказательств в криминалистике.

Мы полагаем, что фиксация информации, которая была размещена в сети Интернет, должна соответствовать некоторым критериям, среди которых нам хотелось бы выделить следующие:

1) Привлечение понятых с последующим разъяснения сущности имеющихся доказательств, технических деталей и использованной специальной терминологии.

2) Описание в протоколе такого следственного действия, как осмотр, информации о содержании и реквизитах информации, представленной в электронной форме.

3) Особое внимание следует уделить записи информации в протоколе браузера – программы, используемой для просмотра веб-контента. Хотя HTML стандартизирован, разные браузеры могут отображать одну и ту же веб-страницу по-разному. Это определяется различиями в принятых стандартах, наличием собственных расширений или интеграцией внешних модулей для обработки веб-контента и отображения результатов. Следовательно, Вы должны правильно указать название и версию браузера, перечислить и описать все пересекающиеся модули (дополнения, расширения).

4) Точное описание деятельности следователя по мониторингу используемого оборудования и программного обеспечения (включая точную версию);

5) Рекомендуется прикрепить (или распечатать, как указано в основном описании протокола) снимки экрана, распечатанные документы, распечатанные результаты внутреннего или внешнего аудита и анализа на сайте.

Заметим, что в случае обнаружения носителя информации, которая была размещена в сети Интернет, необходимо осуществить такие действия, как:

1) исключение доступа к носителю информации лиц, которые не являются участниками следственной группы;

2) проверка электроснабжения объекта, который подлежит осмотру, дабы исключить возможность внезапного прерывания;

3) привлечение специалиста в том случае, если имеются сомнения по поводу уверенности в собственных действиях, так как «специалист в области сетевых технологий сможет должным образом обеспечить контроль над перемещением информации по сети» [14, с. 54];

4) принятие мер, которые имеют своей целью установить логины, пароли и иные пин-коды, необходимые для доступа к программам и базам данных;

5) отключение устройств должно сопровождаться закрытием всех приложений, при этом важно сделать также сделать скриншоты, показывающие насколько велик был список процессов, посредством использования диспетчера задач;

6) проведение осмотра и в дальнейшем фиксации документации, которая находилась рядом с исследуемыми объектами – устройствами.

В протоколе осмотра, изъятия, обыска должны быть определены основные характеристики исследуемых компьютерных устройств:

– внешние признаки каждого устройства;

– компоновка и первоначальное использование (серийность) каждого отдельного устройства с номерами моделей;

– информация на этикетках, наклейках, бирках и бирках производителя.

Также формами допустимой фиксация интернет-информации считаются:

1) Скриншоты, которые предоставляются вместе с рапортом сотрудника.

2) Протокол осмотра источника, на котором размещена информация, представляющая интерес для расследования.

Указанная нами информация может выступать как доказательство в уголовном деле, но при соблюдении всех перечисленных условий.

Следует обратить внимание на то, что CD, DVD, Blue-ray диски должны быть упакованы таким образом, чтобы предотвратить повреждение. Внешние жёсткие диски и жёсткие диски от компьютера упаковываются одинаково. Твердотельные носители информации упаковываются в отдельные пластиковые либо же бумажные пакеты.

Анализ судебно-экспертной практики показывает, что из-за сложности дел, связанных с цифровой информацией, а также отсутствия технических знаний в области компьютерных технологий, следователи склонны поручать расследования государственным экспертам, которым также не хватает специалистов. Также немало случаев, когда экспертам задаются вопросы, выходящие за рамки их специальных знаний и требующие проведения более широкого расследования (особенно по уголовным делам, касающимся авторских и других прав интеллектуальной собственности).

Фиксацию цифровых следов рекомендуется производить в следующем порядке [15, с. 44]:

1) Описание.

2) Фотографирование.

3) Изъятие. Для осуществления этого действия исследованию может подлежать как весь объект в целом, но так и его часть.

Таким образом, изъятие электронных носителей информации – довольно сложный и кропотливый процесс, которые зачастую требует наличия определённых знаний и навыков.

В юридической литературе в настоящее время придерживаются мнения, согласно

которому в данном процессе обязательно должен участвовать специалист. Такого же мнения придерживается отечественный законодатель, который в статье 164.1 Уголовно-процессуального кодекса Российской Федерации закрепил отсутствие специалиста в изъятии электронных носителей в качестве признания доказательств в ходе такого следственного действия недопустимыми.

Список использованных источников

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 21.04.2025) // Собрание законодательства Российской Федерации. – 2001. – № 52 (часть I). – Ст. 4921.
2. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.
3. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть I). – Ст. 3448.
4. Приказ Федеральной службы безопасности Российской Федерации от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» // Российская газета. 2000. № 98.
5. Приказ МВД России от 01.04.2014 № 199 «Об утверждении Инструкции о порядке проведения сотрудниками органов внутренних дел Российской Федерации гласного оперативно-розыскного мероприятия обследование помещений, зданий, сооружений, участков местности и транспортных средств и Перечня должностных лиц органов внутренних дел Российской Федерации, уполномоченных издавать распоряжения о проведении гласного, оперативно-розыскного мероприятия, обследование помещений, зданий, сооружений, участков местности и транспортных средств» // Российская газета. – 2014. – № 118.
6. Архипова, Н. А. Особенности обнаружения, изъятия и осмотра средств мобильной связи в процессе раскрытия и расследования преступлений / Н. А. Архипова. – Текст : непосредственный // Сборник материалов криминалистических чтений. – 2012. – № 8. – С. 11-14.
7. Цифровые следы преступлений: монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. – М: Проспект, 2023. – 168 с. – Текст : непосредственный.
8. Васюков, В. Ф. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / В. Ф. Васюков. – Текст : непосредственный // Российский следователь. - 2016. - № 6. - С. 32-39.
9. Вехов, В. Б. Электронные доказательства: проблемы теории и практики / В. Б. Вехов. – Текст : непосредственный // Правопорядок: история, теория, практика. – 2016. – № 4 (11). – С. 46-50.
10. Вехов, В. Б. Электронные документы как доказательства и объекты судебно-экспертного исследования / В. Б. Вехов. – Текст : электронный // Материалы VI Международной научно-практической конференции «Теория и практика судебной экспертизы в современных условиях», посвященной памяти заслуженного юриста РФ, доктора юридических наук, профессора Юрия Кузьмича Орлова (г. Москва, 19-20 января 2017 г.). – М.: Проспект, 2017. – С. 77-81.
11. Галимханов, А. Б. Порядок обнаружения, изъятия и фиксации цифровых следов преступления / А. Б. Галимханов, А. Ф. Халиуллина. – Текст : непосредственный // Правовое государство: теория и практика. – 2020. – №4-2 (62). – С. 40-44.
12. Льянов, М. М. Процесс обнаружения виртуальных следов при расследовании преступлений / М. М. Льянов. – Текст : непосредственный // Юридическая наука и правоохранительная практика. – 2021. – №4. – С. 97-106.
13. Пастухов, П. С. «Электронные доказательства» в нормативной системе уголовно-

процессуальных доказательств / П. С. Пастухов. – Текст : непосредственный // Пермский юридический альманах. – 2019. – №2. – С. 695-707.

14. Семенов, А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации / А. Ю. Семенов. – Текст : непосредственный // Сибирский юридический вестник. – 2004. – № 1. – С. 53-56.

15. Смушкин, А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин. – Текст : непосредственный // Законность. – 2012. – № 8. – С. 43-45.

16. Приговор Индустриального районного суда г. Барнаула Алтайского края от 23.12.2013 по уголовному делу № 1-535/13 // Индустриальный районный суд г. Барнаула Алтайского края. – URL: https://industrialny--alt.sudrf.ru/modules.php?name=sud_delo&srv_num-=1&name_op=case&case_id=310284176&case_uid=9807e54c-bfd9-4001-ad49-5d69ac235d13&d-elo_id=1540006 (дата обращения: 02.04.2025).

17. Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22-4229/2016 // СПС Гарант. – URL: https://base.garant.ru/144577943/ (дата обращения: 02.04.2025).

Сведения об авторах

Маевский Сергей Сергеевич - кандидат юридических наук, доцент кафедры уголовно-правовых дисциплин, теории и истории государства и права Брянского государственного университета имени академика И.Г. Петровского. Телефон рабочий. +7-4832-58-05-16, e-mail: stelgood@mail.ru

Зайцева Александра Николаевна - студентка 1 курса магистратуры кафедры уголовно-правовых дисциплин, теории и истории государства и права Брянского государственного университета имени академика И.Г. Петровского. E-mail: Sasha_Zayceva05@mail.ru.

UDC 343.13

FORENSIC TECHNOLOGIES FOR DETECTING, RECORDING, AND REMOVING DIGITAL TRACES OF CRIME

Mayevsky S.S., Zaitseva A.N.

Bryansk State Academician I.G. Petrovski University, Bryansk

The article is devoted to the analysis of electronic evidence in the criminal process of the Russian Federation. The legal bases of their use, methods of fixation and features of procedural registration are considered. The requirements for working with electronic media, the role of specialists and judicial practice are highlighted. Special attention is paid to the issues of the permissibility of digital data, their safety and interpretation. The material is relevant for law enforcement officers who are faced with the investigation of cybercrimes and the use of modern technologies in criminal proceedings.

Keywords: electronic evidence, criminal procedure, digital traces, criminalistics, Criminal Procedure Code of the Russian Federation, judicial practice, information technology, material media, operational investigative measures.

References

1. The Criminal Procedure Code of the Russian Federation dated December 18, 2001, No. 174-FZ (as amended on April 21, 2025) // Collection of Legislation of the Russian Federation. – 2001. – No. 52 (part I). 4921.

2. Federal Law No. 144-FZ of 08/12/1995 (as amended on 12/29/2022) "On Operational Investigative activities" // Collection of Legislation of the Russian Federation. – 1995. – No. 33. – Art. 3349.

3. Federal Law No. 149-FZ of 27.07.2006 (as amended on 11/23/2024) "On Information, information Technologies and information Protection" // Collection of Legislation of the Russian Federation. – 2006. – No. 31 (part I). – Art. 3448.

4. Order of the Federal Security Service of the Russian Federation dated 11/13/1999 No. 564

"On Approval of the Regulations on the Certification System of Information Security Equipment for Security Requirements for Information Constituting a State Secret and on its marks of Conformity" // Rossiyskaya Gazeta. 2000. № 98.

5. Order of the Ministry of Internal Affairs of the Russian Federation dated 04/01/2014 No. 199 "On Approval of the Instructions on the Procedure for Conducting a Public Operational Search Event by Employees of the Internal Affairs Bodies of the Russian Federation to Inspect Premises, Buildings, Structures, Terrain and Vehicles and the List of Officials of the internal affairs bodies of the Russian Federation authorized to issue orders on conducting a public, operational search event, inspection of premises, buildings, structures, terrain and vehicles" // Rossiyskaya Gazeta. – 2014. – № 118.

6. Arkhipova, N. A. Features of detection, seizure and inspection of mobile communications equipment in the process of disclosure and investigation of crimes / N. A. Arkhipova. – Text : direct // Collection of materials of criminalistic readings. – 2012. – No. 8. – pp. 11-14.

7. Digital traces of crimes: a monograph / A.M. Bagmet, V. V. Bychkov, S. Yu. Skobelin, N. N. Ilyin. – Moscow: Prospekt, 2023. – 168 p. – Text : immediate.

8. Vasyukov, V. F. Seizure of electronic media in the investigation of crimes: unresolved problems of legal regulation and law enforcement / V. F. Vasyukov. – Text : direct // A Russian investigator. 2016. No. 6. pp. 32-39.

9. Vekhov, V. B. Electronic evidence: problems of theory and practice / V. B. Vekhov. – Text : direct // Law and order: history, theory, practice. – 2016. – № 4 (11). – C. 46-50.

10. Vekhov, V. B. Electronic documents as evidence and objects of forensic expert research / V. B. Vekhov. – Text : electronic // Proceedings of the VI International Scientific and Practical Conference "Theory and practice of forensic examination in modern conditions", dedicated to the memory of Honored Lawyer of the Russian Federation, Doctor of Law, Professor Yuri Kuzmich Orlov (Moscow, January 19-20, 2017). Moscow: Prospekt, 2017. pp. 77-81.

11. Galimkhanov, A. B. The procedure for detecting, removing and fixing digital traces of a crime / A. B. Galimkhanov, A. F. Khaliullina. – Text : direct // The rule of law: theory and practice. – 2020. – №4-2 (62). – Pp. 40-44.

12. Lyanov, M. M. The process of detecting virtual traces in the investigation of crimes / M. M. Lyanov. – Text : direct // Legal science and law enforcement practice. - 2021. – No. 4. – pp. 97-106.

13. Pastukhov, P. S. "Electronic evidence" in the normative system of criminal procedural evidence / P. S. Pastukhov. – Text : direct // Perm Law Almanac. 2019. No. 2. pp. 695-707.

14. Semenov, A. Y. Some aspects of the identification, seizure and investigation of traces arising from the commission of crimes in the field of computer information / A. Y. Semenov. – Text : direct // Siberian Law Bulletin, 2004, No. 1, pp. 53-56.

15. Smushkin, A. B. Virtual footprints in criminology / A. B. Smushkin. – Text : immediate // Legality. – 2012. – No. 8. – pp. 43-45.

16. Verdict of the Industrial District Court of Barnaul, Altai Territory dated December 23, 2013 in the criminal case no. 1-535/13 // Industrial District Court of Barnaul, Altai Territory. – URL: https://industrialny--alt.sudrf.ru/modules.php?name=sud_delo&srv_num-=1&name_op=case&case_id=310284176&case_uid=9807e54c-bfd9-4001-ad49-5d69ac235d13&d-elo_id=1540006 (date of request: 04/02/2025).

17. The appeal ruling of the Judicial Board for Criminal Cases of the Orenburg Regional Court dated 03.11.2016 in case No. 22-4229/2016 // SPS Garant. – URL: https://base .garant.ru/144577943 / (date of access: 04/02/2025).

Author`s information

Mayevsky Sergey Sergeevich - PhD in Law, Associate Professor of the Department of Criminal Law, Theory and History of State and Law, Bryansk State University named after Academician I.G. Petrovsky. Work phone: +7-4832-58-05-16, e-mail: stelgood@mail.ru

Zayceva Alexandra Nikolaevna - 1st year graduate student of the Department of Criminal Law, Theory and History of State and Law of Bryansk State University named after Academician I.G. Petrovsky. E-mail: Sasha_Zayceva05@mail.ru.