

Научная статья
УДК 343.132:[002:004](470)

Мелия Каюмовна Нуркаева
*Уфимский юридический институт МВД Рос-
сии, Уфа, Россия, melia180955@mail.ru*

НЕКОТОРЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ НОВЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ, НАПРАВЛЕННЫХ НА ПОЛУЧЕНИЕ ЦИФРОВОЙ ИНФОРМАЦИИ

Аннотация. Исследование посвящено проблеме достаточности средств доказывания по уголовным делам в эпоху тотальной цифровизации общества. Во вводной части на основе приведенных сведений обозначается актуальность выбранной темы. Автор отметил, что имеющиеся различия в определении природы цифровой информации со стороны ученых наложили определенный отпечаток не только на представления о доказательствах, о средствах доказывания среди практических работников, но и на состояние уголовно-процессуального законодательства. Содержанием работы выступает изучение проблем и перспектив формирования новых следственных действий, направленных на получение цифровой информации. В заключительной части статьи подводятся итоги, формулируются выводы о важности обновления терминологии и понимания характеристик цифровой информации для ее эффективного использования в уголовном судопроизводстве; о совершенствовании программного обеспечения для проведения видео-конференц-связи на стадии предварительного расследования; о необходимости уточнения понятия «электронный носитель информации»; о новом подходе к пониманию следственных действий; о внедрении единого следственного действия, направленного на контроль средств электросвязи.

Ключевые слова: цифровая информация, компьютерная информация, новые следственные действия, комплексные следственные действия, проблемы в области применения исследуемых следственных действий

Для цитирования: Нуркаева М. К. Некоторые проблемы и перспективы формирования новых следственных действий, направленных на получение цифровой информации // Общество, право, государственность: ретроспектива и перспектива. 2025. № 2 (22). С. 43–52.

Original article

Melia K. Nurkaeva
*Ufa Law Institute of the Ministry of Internal Affairs
of Russia, Ufa, Russia, melia180955@mail.ru*

SOME PROBLEMS AND PROSPECTS FOR THE FORMATION OF NEW INVESTIGATIVE ACTIONS AIMED AT OBTAINING DIGITAL INFORMATION

Abstract. The study is devoted to the problem of sufficiency of means of proof in criminal cases in the era of total digitalization of society. In the introductory part, the relevance of the selected topic is indicated based on the information provided. The author noted that the existing differences in the definition of the nature of digital information given by scientists have left their mark not only on the presentation of evidence, on the means of proof among practitioners, but also on the state of criminal procedural law. The content of the work is to study the problems and prospects of forming new investigative actions aimed at obtaining digital information. The final part of the article summarizes the results and formulates conclusions on the importance of updating terminology and understanding the characteristics of digital information for its effective use in criminal proceedings; on improving software for video conferencing during the preliminary investigation phase; on the need to clarify the concept of “electronic information carrier”; on a new approach

to understanding investigative actions; on the introduction of a single investigative action aimed at controlling means of telecommunication.

Keywords: digital information, computer information, new investigative actions, complex investigative actions, problems in the field of application of the investigative actions under study

For citation: Nurkaeva M. K. Some problems and prospects for the formation of new investigative actions aimed at obtaining digital information // Society, law, statehood: retrospective and perspective. 2025. No. 2 (22). P. 43–52. (In Russ.)

Введение

Актуальность темы исследования определяется прежде всего тем, что в связи с прогрессом научно-технических инноваций большая часть современной информации находится в цифровом формате, что является частью глобального тренда к увеличению ее объема. Цифровые данные могут быть как объектом преступлений, так и важным элементом в их расследовании. Например, основные средства коммуникации включают использование мобильных устройств и компьютеров, а транзакции и платежи часто осуществляются через интернет-банкинг¹. Как видим, измененная реальность, а именно цифровизация общества и необходимость повышения эффективности деятельности должностных лиц, осуществляющих доказывание по уголовным делам, по преступлениям, совершаемым с использованием цифровых технологий, влияет на процесс уголовно-процессуального доказывания, особенно на формирование новых следственных действий и в конечном итоге на понимание уголовно-процессуальных доказательств.

Электронные документы становятся нормой во многих сферах жизни общества. Эти обстоятельства делают необходимым собирание и документирование цифровой информации в ходе досудебного производства таким образом, чтобы обеспечить ее сохранность, воспроизводимость и проверяемость.

В настоящем исследовании показаны природа цифровой информации, ее признаки и отличие от компьютерной информации, пути изъятия цифровой информации из раз-

личных носителей, которые в процессуальном аспекте объективируются в предусмотренные уголовно-процессуальным законом следственные действия, проблемы в области применения систем видео-конференц-связи при производстве следственных действий и пути их преодоления, нехватка уголовно-процессуальных ресурсов из-за измененной реальности и необходимость введения в Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ) новых следственных действий по собиранию цифровой информации, в частности внедрения единого комплексного следственного действия, направленного на контроль средств электросвязи.

Вопросы, связанные с формированием новых следственных действий, направленных на получение цифровой информации, освещены в работах О. М. Ефремовой [1], Н. А. Зигуры [2], Е. Р. Россинской, Т. А. Саакова [3], А. И. Зазулина [4], В. Я. Колдина [5], С. С. Алексеева [6], В. Б. Вехова [7], О. Г. Ивановой, П. А. Недбайлова [8], Д. В. Овсянниковой [9], Ю. А. Телевицкой [10], А. Б. Смушкина [11], А. А. Балашовой [12], Х. Х. Рамалданова [13], А. С. Александрова [14], Ю. С. Тютеревой [15], К. С. Плахоты [16], А. Е. Федуловой [17] и других ученых.

Методы

Посредством использования общетеоретических и специально-юридических методов познания, выработанных и апробированных юридической наукой (диалектического, сравнительно-правового методов, метода анализа и систематизации судебной практики и т. д.), автором предпринята попытка анализа трудов ученых в области

¹ Интернет-банкинг – общее название технологий дистанционного банковского обслуживания, а также доступ к счетам и операциям (по ним), предоставляющийся в любое время и с любого устройства, имеющего доступ в Интернет // Википедия. URL: <https://ru.wikipedia.org/wiki/> (дата обращения: 25.03.2025).

права, а также норм действующего законодательства и материалов судебной практики.

Результаты

Изучая влияние цифровизации общества на процесс уголовно-процессуального доказывания и особо на формирование новых следственных действий, автор отметил, что имеющиеся различия в определении природы цифровой информации со стороны ученых наложили свой отпечаток не только на представления о доказательствах, о средствах доказывания среди практических работников, но и на состояние уголовно-процессуального законодательства. Решение теоретических проблем, несомненно, влияет и на законодателя. Закон не есть что-то неизменное, по мере развития науки развивается и он. В соответствии с этим многие ученые, исходя из своего понимания природы цифровой информации, предлагают свои варианты редакций отдельных статей. Поэтому от того, насколько обоснованно будут их взгляды, зависит в конечном счете и теоретический уровень нашего закона.

Обсуждение

Хотя словосочетание «цифровая информация» отсутствует в законодательстве, но в примечании к ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ) детерминирована компьютерная информация как сведения (сообщения, данные), передаваемые в форме электрических сигналов, независимо от способа их хранения и передачи¹. В литературе вопрос о соотношении компьютерной информации и цифровой решается по-разному. Одни используют слова «компьютерная» и «цифровая» как синонимы [1, с. 39–40], другие – нет [2, с. 13–14; 3, с. 112]. Мы не можем поставить знак равенства между компьютерной информацией и цифровой, так как законодательное раскрытие сущности первой информации является узкоспециализированной и не учитывает всех особенностей цифровой информации,

таких как ее существование исключительно в цифровой среде и передача ее с использованием электромагнитных сигналов [4, с. 87]. Информация доступна человеку только через процессы кодирования и декодирования при помощи специализированного оборудования и программ [5, с. 97–99].

Современные предложения включают в себя переопределение компьютерной информации как цифровой [4, с. 73–100; 6, с. 232], что более точно отражает природу и характер таких данных. Новый термин подчеркивает не столько оборудование, сколько форму существования информации [4, с. 85–90; 7, с. 638]. Компьютерная информация также может храниться на различных носителях, не ограничиваясь только компьютерными системами.

Цифровая информация обладает уникальными свойствами [1, с. 40–41; 4, с. 88–90; 8, с. 146–147], делающими ее отличной как от материальных, так и от идеальных объектов. Она хранится в памяти устройств, может быть извлечена пользователем, имеющим доступ. Это не является искусственным интеллектом, хотя и демонстрирует сходство с человеческим мозгом в аспектах обработки информации.

Кроме того, цифровая информация может копироваться без потери данных на исходном устройстве, что делает использование термина «копирование» не вполне уместным. Предпочтительнее использовать «дублирование» или «клонирование»². Эти данные могут передаваться автоматически и их происхождение может быть не всегда ясным, что требует специальных методов для идентификации отправителя или создателя.

Таким образом, обновление терминологии и понимание характеристик цифровой информации критически важны для ее эффективного использования в уголовном судопроизводстве.

В. Б. Вехов обоснованно вводит понятие «электронно-цифровой след», под кото-

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства Рос. Федерации. 1996. № 25, ст. 2954.

² Об отличии копирования и клонирования или дублирования информации см.: [9, с. 11].

рым понимает любую криминалистически значимую компьютерную информацию, то есть сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов. Эти следы являются материальными невидимыми следами. Следы-предметами (частями предметов) и одновременно типичными материальными носителями электронно-цифровых следов следует считать машинные носители информации, интегральные микросхемы, микроконтроллеры, пластиковые карты и другие компьютерные устройства [7, с. 637].

Н. А. Зигура относит к цифровой информации также «набор команд (программ), необходимых для восприятия содержания информации» [2, с. 8]. Однако данные программы лишь создают информацию, обеспечивают ее кодирование, передачу по заданному маршруту, декодирование, но не входят в содержание самой информации.

Цифровая информация имеется на локализованных устройствах, не соединенных в системы (сети). Такими устройствами могут быть отдельные компьютеры, видеокамеры, в том числе встроенные в различные другие устройства (например, мобильные телефоны). Кроме того, информация может быть перенесена на отдельные носители, предназначенные только для хранения и воспроизведения информации, но не для ее создания (оптические диски).

С процессуальной точки зрения важно различать носители, непосредственно содержащие информацию (например, компьютер, на жестком диске которого созданы файлы), и носители, лишь обеспечивающие прием информации с другого источника (например, компьютер, с помощью которого информация запрашивается и принимается с сервера). В первом случае местом производства следственного действия будет место нахождения устройства. Во втором случае это не очевидно.

Законодателю следует определить, что считать местом производства следствен-

ного действия: место непосредственного получения информации или место ее хранения, которое может находиться за пределами Российской Федерации. От решения этого вопроса зависит порядок получения разрешения на проведение следственного действия. Представляется, что местом производства следственного действия при нахождении цифровой информации в удаленном доступе является место нахождения окончательного устройства, с помощью которого будет получаться информация.

Учитывая, что в подобных случаях местом нахождения информации (то есть местом расположения сервера) может быть жилище и на момент проведения следственного действия это неизвестно, для получения цифровой информации в удаленном доступе требуется судебное решение.

На современном этапе цифровая информация изымается двумя способами: либо путем изъятия устройства (ч. 1 ст. 164.1 УПК РФ), на котором находится информация, либо путем копирования информации и переноса ее на носитель, приобретаемый к уголовному делу (ч. 2, 3 ст. 164.1 УПК РФ). В процессуальном аспекте эти два способа изъятия цифровой информации объективируются в различные предусмотренные уголовно-процессуальным законом следственные действия: осмотр, обыск, выемку. В то же время в литературе обосновывается необходимость введения в УПК РФ новых следственных действий по собиранию цифровой информации: осмотра, обыска и выемки в электронных сетях [10, с. 231–232; 11, с. 171]; дистанционного осмотра, обыска информационных ресурсов [12, с. 163–164]; копирования электронной информации [9, с. 151]; контроля электронных отправок и их копирования [11, с. 171]; ареста электронно-почтовой корреспонденции, ее осмотра и копирования [9, с. 151]; получения информации о географических координатах места нахождения (геолокации) абонента, транспортного средства и (или) абонентского устройства [13, с. 192–193]; получения компьютерной информации у операторов связи и организаторов распространения ин-

формации в сети Интернет [1, с. 177–178; 14, с. 133].

Как было отмечено, в современных условиях сохранение перспективного порядка фиксации информации утрачивает актуальность. Ранее существование этого порядка было обусловлено отсутствием у операторов связи прав на сохранение содержания переговоров. В настоящее время, когда фиксация содержания всех переговоров стала обязанностью операторов связи (ст. 64 Федерального закона «О связи» от 7 июля 2003 г. № 126-ФЗ¹), для уголовного судопроизводства требуется только получить от них готовые сведения.

Однако отменять отдельное следственное действие, направленное на получение сведений, передаваемых по средствам связи, и применять для этого выемку [10, с. 189–232; 1, с. 81] или предлагаемое электронно-цифровое копирование (следственное действие общего характера, направленное на изъятие цифровой информации) [1, с. 111–112; 12, с. 161–162] вряд ли целесообразно. Во-первых, требования об обязательном хранении информации, передаваемой с помощью средств электросвязи, уникальны. Во-вторых, тайна связи гарантируется Конституцией Российской Федерации, в силу чего соответствующие сведения выделяются среди других.

Наиболее оптимальным представляется объединение следственных действий, регламентированных ст. 186 и 186.1 УПК РФ, в единое следственное действие («контроль средств электросвязи», «контроль электронных отправок и их копирование») [1, с. 173; 11, с. 171], в рамках которого возможно получение любых сведений о переговорах, ведущихся с использованием средств электросвязи. В УПК РФ необходимо сохранить два порядка получения информации о переговорах: судебный и несудебный. Несудебный порядок целесообразно оставить в качестве исключения: в случаях, когда от потерпевшего поступает заявление об угрозах. Установление спо-

ка получения информации в предлагаемой статье УПК РФ не требуется, поскольку следственное действие будет иметь ретроспективный порядок.

Таким образом, предлагается внедрить единое следственное действие, направленное на контроль средств электросвязи, что упростит и систематизирует процесс получения информации о переговорах, ведущихся с использованием средств электросвязи, обеспечивая при этом соблюдение конституционных гарантий тайны связи и уникальных требований к хранению информации, передаваемой по этим каналам.

По мере появления в нашей повседневной жизни современных информационно-телекоммуникационных технологий сотрудникам правоохранительных органов представилась возможность применять их в ходе расследования преступления и осуществления собирания доказательственной базы.

Однако при использовании видео-конференц-связи в ходе производства таких следственных действий, как очная ставка, допрос, опознание, до сих пор существуют пробелы, связанные с законодательным регулированием процесса организации подобных процессуальных действий [15, с. 100–130; 16, с. 68–90, 113–173]. Их условно можно разделить на две категории: общие и частные, первая из которых относится ко всем вышеперечисленным следственным действиям, вторая – отдельно к конкретному следственному действию. Рассмотрим основные из них.

Общими пробелами в области применения систем видео-конференц-связи при производстве следственных действий являются следующие:

I. Отсутствие программного обеспечения, которое могло бы отвечать всем требованиям, предъявляемым УПК РФ. Так, на сегодняшний день разработана единая система, позволяющая проводить следственные действия посредством видео-кон-

¹ О связи : федер. закон от 7 июля 2003 г. № 126-ФЗ. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

ференц-связи, однако иные альтернативные варианты программ отсутствуют.

На сегодняшний день для производства следственных действий посредством применения системы видео-конференц-связи используется такое программное обеспечение, как сервис видео-конференц-связи МВД России (далее – СВКС-м), который работает на базе информационно-аналитической системы обеспечения деятельности МВД России (далее – ИСОД). Данный продукт разработан для ведомственного использования, следовательно, имеет ряд преимуществ.

Главное преимущество в том, что программа создавалась целенаправленно для системы МВД России, следовательно, в ней заложена высокая защищенность от несанкционированного доступа и утечки информации, а также повышенная устойчивость в работе. СВКС-м – один из сервисов системы ИСОД, обеспечивающий коммуникацию сотрудников с использованием видеосвязи. Он предназначен для оптимизации и ускорения процесса получения и обработки информации при принятии управленческих решений. СВКС-м создавалась для решения следующих задач: обеспечения оперативной связи между сотрудниками и подразделениями МВД России; упрощения процедуры и сокращения командировочных и транспортных расходов при проведении региональных и федеральных совещаний, конференций и семинаров, а также при проведении обучения с использованием системы дистанционных образовательных технологий (СДОТ); повышения производительности труда.

Рассмотрим ее особенности для того, чтобы определить эффективность применения в следственных действиях. Данная программа поддерживает такие типы конференций, как видеозвонок: осуществляется двумя пользователями СВКС-м, при этом оба участника слышат и видят друг друга; групповая видеоконференция (симметричная): групповые конференции создаются администратором на сервере СВКС-м или пользователем СВКС-м (создатель конференции).

Мы считаем, что для проведения следственных действий можно использовать первый тип конференции. Программа имеет физическую защиту в виде авторизации перед входом и началом работы, то есть для входа в приложение программы требуется использовать логин и пароль учетной записи сервиса управления доступом к информационным системам и ресурсам (СУДИС).

Следующей особенностью программы является ее интерфейс, можно сказать, что он выглядит старовато, но при этом он интуитивно понятный, рассчитанный на пользователя средней квалификации. Отметим ряд положительных моментов программы:

1. Во время работы имеется возможность изменять выбор подключенного к компьютеру мультимедийного устройства (громкогоговорителя, микрофона или веб-камеры).

2. Функция записи конференции дает возможность пользователю приложения выполнять видеозаписи в различных режимах.

3. Функция показа презентаций позволяет участникам конференции в отдельном окне демонстрировать слайды: рисунки, фотографии, диаграммы.

4. Функция «электронная доска» дает возможность участникам видеозвонка в отдельном окне рисовать, вводить и редактировать текстовые или графические данные и демонстрировать изображение абоненту.

5. Функция чата позволяет обмениваться текстовыми сообщениями с одним или несколькими абонентами.

6. Функция передачи файлов дает возможность обмениваться файлами непосредственно во время сеанса видеосвязи.

Мы можем сделать вывод о том, что СВКС-м является приоритетной программой для использования в проведении следственных действий. Программа отвечает всем параметрам безопасности, имеет повышенную производительность, что обеспечивает бесперебойность в работе, а также дополнительные функции. Однако необходимо разработать дополнительную программу, которую возможно было бы применять в случаях неисправности основной программы СВКС-м.

II. Недостаточность материально-технической обеспеченности следователей и дознавателей, которых наделили правом использовать системы видео-конференц-связи для реализации уголовно-процессуальных задач. Иными словами, не каждый персональный компьютер органа предварительного расследования сможет поддерживать специальные программы для этих действий.

III. Нестабильность технических средств связи, используемых при производстве следственных действий. Часто возникают постоянные обрывы связи, плохая слышимость, а также иные технические сбои, которые не позволяют качественно осуществлять запись следственного действия и фиксировать ее результат. Это говорит о том, что система видео-конференц-связи не может обеспечивать стабильное подключение.

IV. Отсутствие технического программного обеспечения у лиц, участвующих в проведении следственного действия. Следователь может не воспользоваться правом производить какое-либо следственное действие посредством видео-конференц-связи по той причине, что у свидетеля, потерпевшего или иного участника уголовного судопроизводства не будет компьютера, подключенного к сети Интернет.

Рассмотрев общие проблемы, имеющиеся в ходе производства следственных действий, перейдем к исследованию частных пробелов, которые существуют при производстве отдельных следственных действий.

Одним из пробелов очной ставки является недостаточное использование следователем научно-технических средств – звуко- и видеозаписи, что непосредственно отражается на ее результативности. Результативность очной ставки зависит и от личного умения, и от опыта, а также от серьезного отношения к подготовке ее проведения следователем.

Отсутствие четкого разъяснения понятия «электронный носитель информации» приводит к тому, что на практике часто возникает вопрос о необходимости выполнения требований, которые содержатся в ч. 2 ст. 164.1 УПК РФ. Это становится особенно важным при решении вопроса о привлечении специалиста для изъятия электронных носителей. Неопределенность в отнесении того или иного устройства к категории электронного носителя находит отражение в противоречивой судебной практике. Суды по-разному решают вопрос об отнесении того или иного устройства к категории электронных носителей информации¹.

Таким образом, возникает необходимость в уточнении данного понятия. Большинство авторов научных работ на эту тему отстаивают широкий подход к определению понятия «электронный носитель информации» [10, с. 125–126; 12, с. 20–41; 17, с. 93–94], в соответствии с которым под последним понимаются любые материальные носители информации в цифровом формате, как внешние, так и являющиеся составной частью электронного устройства.

При производстве такого следственного действия, как опознание, посредством системы видео-конференц-связи возникают проблемные аспекты, связанные с отсутствием законодательного регулирования.

На данный момент обозначенные проблемы остаются нерешенными. Однако считаем, что имеющийся функционал в действующей системе видео-конференц-связи СВКС-м дает возможности для проведения опознания. Так, функции записи экрана, показа презентаций, передачи файлов играют особую роль при проведении следственных действий с использованием СВКС-м. Во-первых, запись экрана обеспечит законность выполнения следственных дей-

¹ Апелляционное постановление суда Ханты-Мансийского автономного округа – Югры № 22К-1149-2020 от 10 авг. 2020 г. // Судебные и нормативные акты РФ. URL: <https://sudact.ru> (дата обращения: 25.03.2025) ; Апелляционное постановление Приморского краевого суда № 22-4430/2019 от 28 окт. 2019 г. // Судебные и нормативные акты РФ. URL: <https://sudact.ru> (дата обращения: 25.03.2025) ; Апелляционное постановление Московского областного суда № 22К-4272/2019 от 2 июля 2019 г. // Судебные и нормативные акты РФ. URL: <https://sudact.ru> (дата обращения: 25.03.2025).

ствий и соблюдения ч. 4 ст. 189.1 УПК РФ. Во-вторых, показ презентаций, включая фотографии, имеет важное значение при проведении опознания. Следователь сможет предъявить предметы в режиме реального времени, загрузив фотографии, тем самым предоставить лицу фотографии предметов для опознания. При помощи функции передачи файлов следователь, в производстве которого находится уголовное дело, в ходе допроса имеет возможность оперативно получать документы от участника следственного действия либо отправлять документы для уточнения каких-либо обстоятельств по уголовному делу.

Рассматривая вопрос относительно программного обеспечения для проведения видео-конференц-связи на стадии предварительного расследования, можем сказать, что требуется огромное количество доработок в области программного обеспечения на государственном уровне с последующим закреплением в законодательстве. С одной стороны, законодатель не ограничил должностное лицо в выборе программ, что дает им больше возможностей при производстве следственных действий путем выбора наиболее удобного и стабильного в работе программного обеспечения, с другой – снижается вероятность кибератак, так как наличие боль-

шого количества программ рассеивает внимание преступников и не показывает данные точного места, куда необходимо нанести кибератаку для срыва следственного действия.

Заключение

В результате исследования мы пришли к следующим выводам: о важности обновления терминологии и понимания характеристик цифровой информации для ее эффективного использования в уголовном судопроизводстве; о совершенствовании программного обеспечения для проведения видео-конференц-связи на стадии предварительного расследования; о необходимости уточнения понятия «электронный носитель информации», что имеет значение для определения места производства следственного действия и порядка получения разрешения на его проведение; о новом подходе к пониманию следственных действий; о внедрении единого следственного действия, направленного на контроль средств электросвязи, что упростит и систематизирует процесс получения информации о переговорах, ведущихся с использованием средств электросвязи, обеспечивая при этом соблюдение конституционных гарантий тайны связи и уникальных требований к хранению информации, передаваемой по этим каналам.

СПИСОК ИСТОЧНИКОВ

1. Ефремова О. М. Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве следственных действий : дис. ... канд. юрид. наук. Орел, 2021. 225 с.
2. Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе : дис. ... канд. юрид. наук. Челябинск, 2010. 21 с.
3. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123. DOI: <https://doi.org/10.24411/2587-9820-2020-10060>
4. Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу : дис. ... канд. юрид. наук. Екатеринбург, 2018. 251 с.
5. Колдин В. Я. Электронная информация в праве // Вестник Московского университета. Сер. 11: Право. 2016. № 2. С. 96–110.
6. Алексеев С. С. К вопросу о понятии «цифровая информация» применительно к уголовному судопроизводству // Вестник Университета имени О. Е. Кутафина (МГЮА). 2024. № 1. С. 225–234. DOI: <https://doi.org/10.17803/2311-5998.2024.113.1.225-234>

7. Вехов В. Б. Преступления в сфере цифровой экономики: совершенствование расследования на основе положений электронной криминалистики // Пермский юридический альманах. 2019. № 2. С. 630–640.
8. Иванова О. Г., Недбайлов П. А. Цифровая информация и ее место в уголовно-процессуальном доказывании // Вестник Сибирского юридического института МВД России. 2022. № 2 (47). С. 144–149.
9. Овсянников Д. В. Копирование электронной информации как средство уголовно-процессуального доказывания : дис. ... канд. юрид. наук. Челябинск, 2015. 193 с.
10. Телевицкая Ю. А. Выемка электронных носителей информации по уголовным делам : дис. ... канд. юрид. наук. Н. Новгород, 2023. 330 с.
11. Смушкин А. Б. Концепция «электронных» следственных действий // Криминалистика: вчера, сегодня, завтра. 2021. Т. 19, № 3. С. 165–172. DOI: <https://doi.org/10.24412/2587-9820-2021-3-165-172>
12. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. ... канд. юрид. наук. М., 2020. 216 с.
13. Рамалданов Х. Х. Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений : дис. ... канд. юрид. наук. М., 2024. 244 с.
14. Александров А. С. Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 130–139.
15. Тютерева Ю. С. Дистанционный порядок производства по уголовному делу : дис. ... канд. юрид. наук. М., 2024. 263 с.
16. Плахота К. С. Использование электронных средств связи в уголовном судопроизводстве : дис.... канд. юрид. наук. М., 2023. 269 с.
17. Федулова А. Е. Электронные носители информации в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2022. № 2 (60). С. 90–100.

REFERENCES

1. Yefremova O. M. Implementation of an investigator's authorities aimed at obtaining and using of computer information in the course of investigative procedures : diss. ... Cand. of Law. Orel, 2021. 225 p. (In Russ.)
2. Zigura N. A. Computer information as a form of evidence in the criminal procedure : diss. ... Cand. of Law. Chelyabinsk, 2010. 21 p. (In Russ.)
3. Rossinskaya Ye. R., Saakov T. A. The problems of collecting digital footprints of crimes in social networks and messengers // Forensics: yesterday, today, tomorrow. 2020. No. 3 (15). P. 106–123. DOI: <https://doi.org/10.24411/2587-9820-2020-10060> (In Russ.)
4. Zazulin A. I. Legal and methodological foundations for the use of digital information while establishing evidence in a criminal case : diss. ... Cand. of Law. Yekaterinburg, 2018. 251 p. (In Russ.)
5. Koldin V. YA. Electronic information in law // Bulletin of Moscow University. Series 11. Law. 2016. No. 2. P. 96–110. (In Russ.)
6. Alekseev S. S. On the issue of the concept of “digital information” in relation to criminal proceedings // Bulletin of Moscow State Law University named after O.E. Kutafin (MSAL). 2024. No. 1. P. 225–234. DOI: <https://doi.org/10.17803/2311-5998.2024.113.1.225-234> (In Russ.)
7. Vehov V. B. Crimes in the sphere of digital economy: improvement of investigation on the basis of electronic forensics // Perm legal almanac. 2019. No. 2. P. 630–640. (In Russ.)
8. Ivanova O. G., Nedbailov P. A. Digital information and its place in criminal procedure proof // Bulletin of the Siberian Law Institute of the MIA of Russia. 2022. No. 2 (47). P. 144–149. (In Russ.)
9. Ovsyannikov D. V. Copying of the electronic information as a means in criminal procedure proof : diss. ... Cand. of Law. Chelyabinsk, 2015. 193 p. (In Russ.)
10. Televitskaya Yu. A. Seizure of electronic media in criminal cases : diss. ... Cand. of Law. Nizhny Novgorod, 2023. 330 p. (In Russ.)
11. Smushkin A. B. The concept of “electronic” investigative actions // Forensics: yesterday, today, tomorrow. 2021. Vol. 19, No. 3. P. 165–172. DOI: <https://doi.org/10.24412/2587-9820-2021-3-165-172> (In Russ.)

12. Balashova A. A. Electronic media and their use in criminal procedure proof : diss. ... Cand. of Law. Moscow, 2020. 216 p. (In Russ.)
13. Ramaldanov Kh. Kh. The process of proof in criminal cases in the context of total digitalization of public relations : diss. ... Cand. of Law. Moscow, 2024. 244 p. (In Russ.)
14. Aleksandrov A. S. The problems of the theory of criminal procedural proof, which must be solved in connection with the transition to the digital age // Judicial authority and criminal process. 2018. No. 2. P. 130–139. (In Russ.)
15. Tyutereva Yu. S. Remote procedure for criminal proceedings : diss. ... Cand. of Law. Moscow, 2024. 263 p. (In Russ.)
16. Plakhota K. S. The use of electronic means of communication in criminal proceedings : diss. ... Cand. of Law. Moscow, 2023. 269 p. (In Russ.)
17. Fedulova A. E. Electronic data carriers in the criminal proceedings // Legal science and law enforcement practice. 2022. No. 2 (60). P. 90–100. (In Russ.)

Информация об авторе:

Нуркаева М. К. – кандидат юридических наук.

Information about the author:

Nurkayeva M. K. – Candidate of Law.

Статья поступила в редакцию 04.04.2025; одобрена после рецензирования 09.04.2025; принята к публикации 20.06.2025.

The article was submitted 04.04.2025; approved after reviewing 09.04.2025; accepted for publication 20.06.2025.