Научная статья
УДК: 343.985.2

ПОНЯТИЕ И ВИДЫ ЦИФРОВОЙ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Виталий Федорович Васюков[1], Эмин Исахан оглы Дамирчиев[2]
[1]Московская академия Следственного комитета Российской Федерации имени А. Я. Сухарева, г. Москва, Российская Федерация, vvf0109@yandex.ru
[2]Московский государственный институт международных отношений МИД России (МГИМО), г. Москва, Российская Федерация damirchiyev@mail.ru

Аннотация. XXI век характеризуется развитием «информационной» цивилизации, в связи с чем «информация» как продукт жизнедеятельности приобретает огромное значение, а цифровая форма ее формирования, накопления и передачи значительно расширяет возможности использования в различных сферах деятельности, в том числе и правоприменительной. В этой связи вопросы использования цифровой информации в уголовном судопроизводстве являются весьма актуальными, поскольку в правоприменительной практике сегодня остро стоит вопрос о необходимости совершенствования процессуально-правовой формы закрепления «цифровой информации» как доказательства. В статье на основе понятия, видов и особенностей цифровой информации исследуются отдельные вопросы ее использования в качестве доказательств. Особое внимание уделено разновидностям цифровой информации, таким как пользовательские данные, системные логи, метаданные и телекоммуникационные сведения, а также их доказательственной ценности.

Ключевые слова: цифровая информация, доказывание, уголовное дело, электронный носитель, расследование

Для цитирования: Васюков, В. Ф., Дамирчиев, Э. И. Понятие и виды цифровой информации, используемой в доказывании по уголовным делам // Криминалистика: вчера, сегодня, завтра. 2025. Т. 34. № 2. С. 38–50.

CONCEPT AND TYPES OF DIGITAL INFORMATION USED IN EVIDENCE IN CRIMINAL CASES

Vitaly F. Vasyukov[1], Emin Is. oglu Damirchiyev[2]
[1]Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev, Moscow, Russian Federation, vvf0109@yandex.ru
[2]Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO), Moscow, Russian Federation, damirchiyev@mail.ru

Abstract. The 21st century is characterized by the development of an "information" civilization, in connection with which "information" as a product of life activity acquires enormous significance, and the digital form of its formation, accumulation and transmission significantly expands the possibilities of use in various spheres of activity, including law enforcement. In this regard, the issues of using digital information in criminal proceedings are very relevant, since in law enforcement practice today there is an acute issue of the need to improve the procedural and legal form of securing "digital information" as evidence. The article examines individual issues of its use as evidence based on the concept, types and characteristics of digital information. Particular attention is paid to the types of digital information, such as user data, system logs, metadata and telecommunications information, as well as their evidentiary value.

Keywords: digital information, evidence, criminal case, electronic media, investigation

For citation: Vasyukov, V. F., Damirchiyev, E. I. Ponyatie i vidy cifrovoj informacii, ispol'zuemoj v dokazyvanii po ugolovnym delam [Concept and types of digital information used in evidence in criminal cases]. Kriminalistika: vchera segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 34, no 2, pp. 38–50 (in Russ.).

Введение

В современном обществе наблюдается стремительное развитие цифровых технологий, оказывающих существенное влияние на все сферы жизни, включая уголовное судопроизводство. В условиях роста числа мошеннических действий с использованием информационно-коммуникационных технологий цифровая информация приобретает ключевое значение для раскрытия и расследования преступлений.

По данным ФСБ России, в 2024 году зарегистрировано более 640 тысяч таких преступлений, а совокупный ущерб составил более 170 млрд рублей. Проведенными мероприятиями было прекращено функционирование незаконного виртуального узла связи, изъято более 1 200 сим-боксов, 1 000 модемов и телефонных аппаратов, 1,2 млн сим-карт, задержано 208 их владельцев. Возбуждено и расследуется более 950 уголовных дел по статьям 205, 159, 272 и 274 УК РФ[1]. Вскрыты факты использования кол-центров для склонения граждан России к совершению диверсий[2].

В таких условиях цифровая информация в доказывании по уголовным делам приобретает главенствующее значение. Она перестает быть вспомогательным элементом, своего рода «довеском» к традиционным видам доказательств, и становится ключевым фактором, определяющим исход уголовного преследования. Цифровая информация в доказывании

[1] Архивные данные официальной статистики ФСБ России.

[2] О противодействии мошеннической деятельности // Федеральная служба безопасности Российской Федерации : офиц. сайт. URL: http://www.fsb.ru/fsb/press/message/single.htm!id=10440275@fsbMessage.html (дата обращения: 16.05.2025).

является не просто ценным ресурсом, а необходимым условием эффективной борьбы с преступностью, защиты прав и свобод граждан и обеспечения национальной безопасности.

Собирание, проверка, оценка и использование доказательств в уголовном процессе играют ключевую роль, поскольку именно на их основе устанавливаются обстоятельства дела, принимаются процессуальные решения и выносятся итоговые судебные решения (п. 33, 53.2 ст. 5 УПК РФ[3]). Между тем доказывание представляет собой особый вид познавательной деятельности, регулируемой законом и осуществляемой уполномоченными субъектами, направленной на установление обстоятельств, входящих в предмет доказывания.

Согласно ст. 74 УПК РФ, доказательствами являются любые сведения, на основе которых суд, прокурор, следователь или дознаватель в установленном порядке определяют наличие или отсутствие значимых для уголовного дела обстоятельств [1, с. 161]. Однако в российском законодательстве отсутствует четкое определение термина, этимологически сопряженного с электронной «начинкой» носителей, которые приобщаются к уголовному делу. Главным образом именно поэтому в современной уголовно-процессуальной доктрине такого рода электронные носители традиционно квалифицируются либо как вещественные доказательства, либо как иные документы, что обусловлено их двойственной природой. Критерий разграничения между этими категориями основывается на классическом доказательственном подходе: если доказательственное значение имеет материальный носитель информации с его физическими свойствами (например, поврежденный жесткий диск или флеш-накопитель со следами взлома), такие объекты следует относить к вещественным доказательствам. Как отмечает Х. Х. Рамалданов, в случаях, когда ценность представляет содержательная составляющая информации (текстовые файлы, базы данных, аудио- и видеозаписи), более обоснованным представляется их отнесение к документальным доказательствам [2, с. 123].

Считаем наиболее приемлемым под цифровой информацией в уголовном судопроизводстве понимать данные, представленные в электронной форме, зафиксированные на материальных носителях или передаваемые через информационно-телекоммуникационные сети, которые могут содержать сведения, имеющие значение для установления обстоятельств уголовного дела.

Основная часть

В отличие от традиционных вещественных доказательств, цифровая информация может су-

[3] Российская Федерация. Законы. Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 22 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 25.04.2025).

ществовать в идентичных копиях, что требует особых механизмов обеспечения ее достоверности и сохранности.

Важным аспектом работы с цифровой информацией является ее зависимость от технических средств обработки и отображения. Одни и те же данные могут интерпретироваться по-разному в зависимости от используемого программного обеспечения, что требует стандартизации методов их анализа. Кроме того, как ранее было отмечено в публикации одного из авторов, цифровая информация отличается высокой степенью изменчивости – она может быть быстро модифицирована или уничтожена, в связи с чем предъявляются особые требования к оперативности проведения следственных действий [3, с. 64].

Особенность цифровой информации как имеющей доказательственное значение заключается в ее принципиально ином генезисе по сравнению с традиционными доказательствами. А. Г. Волеводз и А. Д. Цыплакова отмечают, что в отличие от материальных следов, образующихся под воздействием объективных физических, химических или биологических процессов, электронные данные формируются в результате взаимодействия двух факторов: аппаратной составляющей (физические носители) и программного обеспечения, созданного разработчиками на основе субъективно выбранных алгоритмов» [4, с. 23]. Например, при расследовании киберпреступления важное доказательственное значение могут иметь как сам поврежденный сервер (вещественное доказательство), так и извлеченные с него логи сетевой активности (документальное доказательство), при этом последние формируются по алгоритмам, заложенным программистами в систему логирования.

Подобная двойственная природа цифровой информации, имеющей доказательственное значение, требует особого процессуального подхода к их собиранию, фиксации, при использовании которого правоприменителем должна учитываться как материальная составляющая (физические носители), так и информационная (содержательные данные). В этой связи Е. З. Сидорова и Грибунов О.П. отмечают, что следует учитывать, что программные алгоритмы, определяющие форму и содержание электронных данных, могут быть искажены, что требует дополнительных мер по проверке достоверности таких доказательств [5, с. 18].

Процесс собирания цифровой информации в ходе расследования уголовного дела осуществляется в рамках традиционных следственных действий, однако существуют особые правила, касающиеся только случаев копирования компьютерной информации, а также изъятия носителя, на котором она содержится (ст. 164^1 УПК РФ). При этом основными процессуальными формами получения цифровой информации являются осмотр, обыск и выемка, в ходе которых могут быть обнаружены и изъяты персональные компьютеры, мобильные устройства, внешние накопители (флеш-карты,

съемные жесткие диски) и иные технические средства хранения информации.

Следует согласиться с Е. И. Третьяковой и А. Б. Соколовым, которые отмечают, что при проведении данных следственных действий необходимо учитывать технологические особенности цифровых доказательств: в ходе осмотра компьютерной техники в первую очередь фиксируется состояние подключенных устройств и запущенных процессов, поскольку внезапное отключение питания может привести к потере оперативных данных [6, с. 232]. Особую сложность представляет копирование цифровой информации с серверного оборудования крупных предприятий, функционирующего в круглосуточном режиме, где требуется обеспечить как сохранность доказательств, так и непрерывность работы системы.

Последующая экспертиза изъятых носителей включает создание криминалистических копий с применением аппаратно-программных комплексов, исключающих модификацию исходных данных, что особенно важно при расследовании преступлений в финансовой сфере, где цифровые следы транзакций могут быть ключевыми доказательствами. Проверка достоверности цифровой информации требует комплексного анализа как содержащейся информации, так и метаданных (временных штампов, цифровых подписей, истории изменений), что позволяет установить целостность и неизменность цифровых следов.

Метаданные представляют собой структурированную информацию, описывающую характеристики других данных, и играют ключевую роль в цифровой криминалистике, анализе контента и системном администрировании. В зависимости от типа файла метаданные могут извлекаться из различных источников и использоваться для установления происхождения файла или хронологии событий [7, с. 230].

Одним из наиболее распространенных являются метаданные документов, встроенные в офисные файлы (Word, Excel, PDF) и содержащие данные о пользователе, дате создания, последних изменениях и даже истории правок. Например, документ Microsoft Word может хранить сведения о пользователях, вносивших правки, что позволяет отследить цепочку редактирования. Аналогично PDF-файлы часто содержат метаданные о программе, в которой они были созданы, и даже о принтере, если документ готовился к печати.

Мультимедийные метаданные представляют интерес при изучении фото- и видеоматериалов. Фотографии в форматах JPEG или PNG содержат данные EXIF (Exchangeable Image File Format), включающие параметры съемки (выдержку, диафрагму, ISO), модель камеры или смартфона, а также географические координаты, если геолокация была активна. В случае исследования аудио- и видеофайлов метаданные могут указывать на устройство записи, кодек, длительность и даже программное обеспечение, использованное для монтажа [8].

Сетевые метаданные играют важную роль при анализе интернет-контента. Так, HTML-страницы содержат метатеги, которые определяют описание, ключевые слова, автора и кодировку документа. Кроме того, серверные логи хранят IP-адреса пользователей, время запросов и используемые браузеры, что может быть использовано для анализа поведения в сети.

В электронной переписке метаданные включают не только адреса отправителя и получателя, но и маршрут прохождения письма через серверы, временные метки и даже данные о вложениях. Аналогично в журналах телефонных вызовов фиксируются номера абонентов, длительность разговоров и местоположение базовых станций.

Наконец, системные метаданные формируются операционными системами и файловыми системами. К ним относятся атрибуты файлов (даты создания, изменения и последнего доступа), права доступа, идентификаторы пользователей (UID/GID в Unix-системах), а также журналы событий (например, Windows Event Log). Исследователи отмечают, что эти данные позволяют восстановить хронологию работы с файлами, выявить несанкционированные изменения или установить, какое программное обеспечение взаимодействовало с определенными ресурсами [9, с. 175].

В контексте уголовного судопроизводства цифровая информация, используемая в доказывании, может быть классифицирована по нескольким основаниям, отражающим ее содержательные и технические характеристики. Первостепенное значение имеет разделение информации по ее функциональному назначению в процессе доказывания.

К *первому* виду А. С. Агафонов и А. А. Количенко относят пользовательские данные, которые включают сознательно создаваемую и вводимую пользователем информацию: текстовые документы, электронные письма, сообщения в мессенджерах, записи в базах данных, а также мультимедийный контент (фотографии, аудио- и видеозаписи) [10, с. 47]. Отличительной чертой данного вида информации является ее непосредственная связь с деятельностью субъектов, что обусловливает ее особую значимость при установлении состава преступления.

Так, в ходе оперативно-розыскных мероприятий, направленных на выявление и пресечение деятельности участников запрещенной организации, с жесткого диска компьютера одного из фигурантов были извлечены пользовательские файлы. Анализ этих данных позволил обнаружить текстовые документы, содержащие инструкции по проведению диверсий, а также аудиофайлы с пропагандистскими материалами. Указанные доказательства послужили основанием для предъявления обвинения по ст. 282 УК РФ.

Вторую значимую группу составляют системные данные, формируемые автоматически в процессе функционирования компьютерных систем: логи событий, журналы регистрации, временные метки, параметры системных

настроек. Эти данные обладают высокой доказательственной ценностью при установлении факта несанкционированного доступа, определении временных параметров совершения преступления или восстановлении последовательности действий пользователя. В отличие от пользовательских данных, как отмечают А. Б. Соколов и Е. И. Третьякова, они объективно фиксируют действия системы, что минимизирует риски фальсификации и позволяет точно устанавливать ключевые параметры преступной деятельности [11, с. 220].

Например, в ходе расследования кибератаки на информационную систему одного из министерств специалисты по компьютерной безопасности изучили журналы событий безопасности. В них были зафиксированы зарубежные IP-адреса, с которых осуществлялось подключение, точное время попыток подбора паролей (брутфорс-атаки), изменения в конфигурационных файлах. При этом анализ временных меток позволил установить, что злоумышленник действовал в ночное время, используя уязвимость в системе авторизации. Данные логов стали основой для идентификации подозреваемого через его провайдера.

Особую категорию цифровой информации образуют *данные телекоммуникационных операторов,* включающие сведения о соединениях абонентов, маршрутизации трафика, местоположении устройств. И как верно отмечают Каширгов А. Х. и Семенов Е. А., их значение особенно велико при расследовании преступлений, совершаемых с использованием средств связи, где они позволяют установить круг подозреваемых лиц и реконструировать события [12, с. 310].

Важное место в системе цифровых доказательств занимают данные, извлекаемые из облачных сервисов и интернет-платформ, которые характеризуются распределенным характером хранения и требуют особых процедур получения, включая международное сотрудничество при трансграничном расположении серверов.

Отдельно следует выделить *информацию, получаемую в ходе оперативно-розыскных мероприятий в компьютерных сетях*: перехваченные сообщения, данные о сетевой активности, результаты мониторинга интернет-ресурсов. При работе с каждым из указанных видов цифровой информации необходимо учитывать специфические особенности, определяющие выбор соответствующих процессуальных форм закрепления, что требует от сотрудников правоохранительных органов не только юридических знаний, но и понимания технических аспектов функционирования цифровых систем.

Между тем использование фигурантами специализированного программного обеспечения для безопасных соединений, во-первых, создает серьезные препятствия для идентификации участников организованных групп, которые функционируют с помощью информационных технологий. Во-вторых, использование геолокационных данных и навигационных систем для орга-

низации дистанционного обмена запрещенными к обороту предметами свидетельствует об адаптации преступных схем к современным цифровым технологиям. В-третьих, интеграция криптовалютных платежей в систему оплаты незаконных товаров и услуг, как отмечают авторы, указывает на высокий уровень технологического оснащения организованной преступности, в том числе имеющей транснациональные связи [13, с. 9].

Так, на территории Алтайского края была выявлена преступная группа, специализирующаяся на бесконтактном сбыте синтетических наркотиков через интернет-магазин, функционирующий в мессенджере Telegram и использующий автоматизированные программы для связи с покупателями.

Деятельность группы тщательно конспирировалась и строилась на строгой иерархии. Новые участники проходили отбор, обучение и получали методические рекомендации, охватывающие вопросы создания легенды, выявления слежки, конспирации (использование второго телефона, сменных SIM-карт, общественного Wi-Fi), защиты информации на мобильных устройствах (использование VPN, специальных приложений для координат и меток на фотографиях, очистка переписки и метаданных). Отдельное внимание уделялось инструкциям по поведению при задержании и допросе, включая уничтожение материальных и цифровых следов.

Основой доказательной базы по этому делу стала цифровая информация, том числе переписка в Telegram, фотографии с геолокацией, данные об используемых приложениях и SIM-картах, а также результаты оперативного наблюдения. Совокупность этих доказательств неопровержимо подтвердила систематическую преступную деятельность подсудимого, направленную на сбыт наркотических средств через сеть «Интернет».

Организация группы характеризовалась четким распределением ролей, системой перехода от «розничного» закладчика к «оптовому», беспрекословным подчинением, жестким контролем качества работы (соблюдение правил, система поощрений и наказаний, отчетность). Оплата труда производилась криптовалютой через цепочку транзакций с компенсацией расходов на проживание, упаковку и транспорт. Схема сбыта включала в себя получение наркотиков от «операторов» и размещение закладок с последующей передачей информации. Новые закладчики получали небольшие партии, которые увеличивались по мере успешной работы.

Доказательствами по уголовному делу стали сведения, полученные из электронных носителей информации. В ходе проведения оперативно-розыскных мероприятий и следственных действий была зафиксирована переписка между подозреваемым и куратором магазина, причем предметом переписки стала информация о получении, распространении наркотических средств, инструкции по созданию тайников-закладок, меры конспирации.

Также в ходе осмотра в галерее телефона обнаружены фотографии, содержащие геолокационные данные, полученные через приложение обмена сообщений. Указанные фотографии зафиксировали местоположение тайников с наркотическими средствами[4].

Вопрос изъятия цифровой информации, хранящейся на электронных носителях за пределами национальной юрисдикции, в настоящее время представляет собой одну из наиболее сложных процессуальных и правовых проблем современного уголовного судопроизводства. Как справедливо отмечают О. В. Химичева и А. В. Андреев, отсутствие единого международного нормативного регулирования в данной сфере создает существенные препятствия для эффективного противодействия киберпреступности [14, с. 22].

Сложность заключается в том, что современные информационные технологии позволяют преступникам использовать трансграничную инфраструктуру: регистрировать домены, размещать контент и хранить данные в юрисдикциях, не имеющих договорных обязательств с Российской Федерацией о правовой помощи. В таких случаях традиционные механизмы получения доказательств оказываются неработоспособными.

В качестве возможного решения данной проблемы можно предложить международное сотрудничество через многосторонние соглашения в рамках действующих региональных групп, предусматривающие упрощенные процедуры предоставления цифровых доказательств.

Выводы и заключение

Резюмируя обозначенные вопросы, представляется необходимым отметить, что современное уголовное судопроизводство сталкивается с необходимостью адаптации традиционных процессуальных механизмов к стремительно развивающимся цифровым технологиям. Проведенный анализ позволяет констатировать, что цифровая информация, обладая двойственной природой (материальный носитель и нематериальное содержание), требует разработки специализированных подходов к ее собиранию, фиксации и исследованию. На сегодняшний день в российской правовой системе сохраняется терминологическая и классификационная неопределенность в отношении электронных доказательств, что проявляется в их искусственном подразделении на вещественные доказательства и документы без учета их технологической специфики.

Практика расследования уголовных дел демонстрирует возрастающую доказательственную ценность различных видов цифровой информации – от пользовательских данных и системных логов до метаданных и телекоммуникационных сведений. При этом каждый вид информации требует

[4] Приговор Железнодорожного районного суда г. Барнаула (Алтайский край) от 23 июля 2024 г. по делу № 1-409/2024 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/ (дата обращения: 25.04.2025).

специфических методов извлечения и анализа, что обусловливает необходимость междисциплинарного подхода, сочетающего юридические знания с компетенциями в области информационных технологий.

Особую проблему представляет трансграничный характер формирования цифровых следов, когда криминалистически значимая информация хранится на серверах за пределами национальной юрисдикции. Отсутствие унифицированных международных механизмов получения таких доказательств существенно затрудняет расследование преступлений, в связи с чем представляется необходимым проработка вопроса о возможности заключения международных соглашений, регламентирующих процедуры взаимодействия правоохранительных органов в части получения такой информации.

СПИСОК ИСТОЧНИКОВ

1. *Россинский, С. Б.* Доказательства по уголовному делу: требуется ли вносить коррективы в статью 74 УПК РФ? // Криминалистика: вчера, сегодня, завтра. 2023. № 2 (26). С. 161–171.

2. *Рамалданов, Х. Х.* Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. 2022. № 1 (60). С. 121–128.

3. *Агафонов, А. С., Васюков, В. Ф.* К вопросу об использовании цифровой информации при расследовании преступлений в сфере дорожного движения (на примере Итальянской Республики) // Безопасность дорожного движения. 2025. № 1. С. 62–72.

4. *Волеводз, А. Г., Цыплакова, А. Д.* Цифровые доказательства в уголовном процессе государств – членов совета сотрудничества арабских государств персидского залива: правовой статус и процедуры признания // Вестник экономической безопасности. 2024. № 2. С. 21–29.

5. *Сидорова, Е. З., Грибунов, О. П.* Особенности квалификации и предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий : учеб. пособие. Иркутск : Восточно-Сибирский институт МВД России, 2024. 128 с.

6. *Третьякова, Е. И., Соколов, А. Б.* Допрос специалиста при расследовании преступлений, совершенных с использованием информационных технологий: процессуальные и криминалистические аспекты // Вестник Восточно-Сибирского института МВД России. 2023. № 3 (106). С. 232–243.

7. *Velden, L.* Forensic devices for activism: Metadata tracking and public proof // Big Data & Society. 2015. Т. 2. №. 2. P. 205–243.

8. *Suryal, A.* Leveraging metadata in social media forensic investigations: Unravelling digital clues-A survey study //Forensic Science International: Digital Investigation. 2024. Т. 50.

9. *Apsimet, N. M., Alimkulov, Y. T., Duisenbayeva, G. Z.* The collection of digital traces in the investigation of online crimes // Eurasian National University Law Series. 2024. T. 149. №. 4. P. 170–185.

10. *Агафонов, А. С., Количенко, А. А.* Электронный носитель информации как источник получения электронных доказательств по уголовным делам, связанным с нарушением правил дорожного движения // Безопасность дорожного движения. 2023. № 2. С. 45–49.

11. *Соколов, А. Б., Третьякова, Е. И.* Осмотр мобильного телефона: неразрешенные вопросы правоприменения // Криминалистика: вчера, сегодня, завтра. 2023. № 2 (26). С. 214–228.

12. *Каширгов, А. Х., Семенов, Е. А.* Некоторые вопросы противодействия преступлениям, совершенным с использованием IT-технологий // Евразийский юридический журнал. 2021. № 9 (160). С. 309–310.

13. *Грибунов, О. П., Усачев, С. И., Усачева, Е. А.* Криптовалюта и иные виртуальные активы как феномен современной преступности: проблемы раскрытия, расследования и предупреждения // Российский следователь. 2024. № 4. С. 7–12.

14. *Химичева, О. В., Андреев, А. В.* Цифровизация как тренд развития современного уголовного процесса // Вестник Московского университета МВД России. 2020. № 3. С. 21–23.

REFERENCES

1. *Rossinskij, S.B.* Dokazatel'stva po ugolovnomu delu: trebuetsya li vnosit' korrektivy v stat'yu 74 UPK RF? [Evidence in a criminal case: is it necessary to make adjustments to Article 74 of the Criminal Procedure Code of the Russian Federation?]. Kriminalistika: vchera, segodnya, zavtra – Forensics: yesterday, today, tomorrow. 2023, no. 2 (26), pp. 161-171. (in Russian).

2. *Ramaldanov, H.H.* Ponyatie i sushchnost' cifrovizacii dokazatel'stv i dokazyvaniya v ugolovnom sudoproizvodstve [Concept and essence of digitalization of evidence and proving in criminal proceedings]. Vestnik Volgogradskoj akademii MVD Rossii – Vestnik of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2022, no. 1 (60), pp. 121-128. (in Russian).

3. *Agafonov, A. S., Vasyukov, V. F.* K voprosu ob ispol'zovanii cifrovoj informacii pri rassledovanii prestuplenij v sfere dorozhnogo dvizheniya (na primere Ital'yanskoj Respubliki) [On the issue of using digital information in investigating crimes in the field of road traffic (on the example of the Italian Republic)]. Bezopasnost' dorozhnogo dvizheniya – Road safety. 2025, no. 1, pp. 62-72. (in Russian).

4. *Volevodz A.G., Cyplakova A.D.* Cifrovye dokazatel'stva v ugolovnom processe gosudarstv - chlenov soveta sotrudnichestva arabskih gosudarstv persidskogo zaliva: pravovoj status i procedury priznaniya [Digital evidence in criminal proceedings of the member states of the Cooperation Council for the Arab States of the Persian Gulf: legal status and recognition procedures]. Vestnik

ekonomicheskoj bezopasnosti – Economic Security vestnik. 2024, no. 2, pp. 21–29. (in Russian).

5. *Sidorova, E. Z., Gribunov, O. P.* Osobennosti kvalifikacii i preduprezhdeniya prestuplenij, sovershaemyh s ispol'zovaniem informacionnyh (cifrovyh) tekhnologij [Features of qualification and prevention of crimes committed with the use of information (digital) technologies]. Irkutsk, 202,. 128 p. (in Russian).

6. *Tret'yakova, E. I., Sokolov A.B.* Dopros specialista pri rassledovanii prestuplenij, sovershennyh s ispol'zovaniem informacionnyh tekhnologij: processual'nye i kriminalisticheskie aspekty [Interrogation of a specialist in the investigation of crimes committed using information technologies: procedural and forensic aspects]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2023, no. 3(106), pp. 232-243. (in Russian).

7. *Velden, L.* Forensic devices for activism: Metadata tracking and public proof. Big Data & Society. 2015, vol. 2, no. 2, pp. 205-243.

8. *Suryal, A.* Leveraging metadata in social media forensic investigations: Unravelling digital clues-A survey study. Forensic Science International: Digital Investigation. 2024, T. 50.

9. *Apsimet, N. M., Alimkulov, Y. T., Duisenbayeva, G. Z.* The collection of digital traces in the investigation of online crimes. Eurasian National University Law Series. 2024, vol. 149, no. 4, pp. 170-185.

10. *Agafonov, A.S., Kolichenko, A.A.* Elektronnyj nositel' informacii kak istochnik polucheniya elektronnyh dokazatel'stv po ugolovnym delam, svyazannym s narusheniem pravil dorozhnogo dvizheniya [Electronic storage medium as a source of obtaining electronic evidence in criminal cases related to violation of traffic rules]. Bezopasnost' dorozhnogo dvizheniya – Road safety. 2023, no. 2, pp. 45-49. (in Russian).

11. *Sokolov, A. B., Tret'yakova, E.I*. Osmotr mobil'nogo telefona: nerazreshennye voprosy pravoprimeneniya [Inspection of a mobile phone: unresolved issues of law enforcement]. Kriminalistika: vchera, segodnya, zavtra – Forensics: yesterday, today, tomorrow. 2023, no. 2(26), pp. 214-228. (in Russian).

12. Kashirgov A.H., Semenov E.A. Nekotorye voprosy protivodejstviya prestupleniyam, sovershennym s ispol'zovaniem IT-tekhnologij [Some issues of counteracting crimes committed using IT technologies]. Evrazijskij yuridicheskij zhurnal – Eurasian Law Journal. 2021, no. 9 (160), pp. 309–310. (in Russian).

13. Gribunov O.P., Usachev S.I., Usacheva E.A. Kriptovalyuta i inye virtual'nye aktivy kak fenomen sovremennoj prestupnosti: problemy raskrytiya, rassledovaniya i preduprezhdeniya [Cryptocurrency and other virtual assets as a phenomenon of modern crime: problems of detection, investigation and prevention]. Rossijskij sledovatel' – Russian investigator. 2024, no. 4, pp. 7-12.

14. Himicheva O.V., Andreev A.V. Cifrovizaciya kak trend razvitiya sovremennogo ugolovnogo processa [Digitalization as a trend in the development of modern criminal proceedings]. Vestnik Moskovskogo universiteta MVD Rossii. Vestnik of the Moscow University of the Ministry of Internal Affairs of Russia. 2020, no. 3, pp. 21-23. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Васюков Виталий Федорович, доктор юридических наук, профессор, главный научный сотрудник научно-исследовательского отдела. Московская академия Следственного комитета Российской Федерации имени А. Я. Сухарева. 125080, Российская Федерация, г. Москва, ул. Врубеля, 12.

Дамирчиев Эмин Исахан оглы, кандидат юридических наук, кандидат политических наук, доцент кафедры уголовного права, уголовного процесса и криминалистики. Московский государственный институт международных отношений МИД России (МГИМО). 119454, Российская Федерация, г. Москва, проспект Вернадского, 76б.

INFORMATION ABOUT THE AUTHORS

Vitaly F. Vasyukov, Doctor of Law, Professor, Chief Researcher of the Research Department of the Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev. 12, Vrubel st., Moscow, Russian Federation, 125080.

Emin Is. oglu Damirchiev, Candidate of Legal Sciences, Candidate of Political Sciences, Associate Professor of the Department of Criminal Law, Criminal Procedure and Forensic Science. Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO), 76 b, Vernadsky Avenue, Moscow , Russian Federation, 119454.