

Original article
УДК 349
DOI 10.33184/pravgos-2025.1.28

Научная статья

ШИХАЛИЕВА Сельджан Заур кызы
Московский государственный юридический
университет имени О.Е. Кутафина (МГЮА),
Москва, Россия,
e-mail: seldjan-sh@mail.ru

SHIKHALIYEVA Seldjan Zaur qizi
Kutafin Moscow State Law University (MSAL),
Moscow, Russia.

ОТСУТСТВИЕ ХЭШ-СУММЫ КАК ПРОЦЕССУАЛЬНАЯ ОШИБКА, ВОЗНИКАЮЩАЯ В СУДЕБНОЙ ЭКСПЕРТИЗЕ ПРИ ИССЛЕДОВАНИИ ОБЪЕКТОВ В ЦИФРОВОЙ ФОРМЕ

THE ABSENCE OF A HASH SUM AS A PROCEDURAL ERROR ARISING IN A FORENSIC
EXAMINATION WHEN ANALYSING OBJECTS IN A DIGITAL FORM

Аннотация. Актуальной задачей при работе с цифровыми объектами является соблюдение процессуальных норм и правил при назначении судебной экспертизы и проведении исследования. Их несоблюдение приводит к совершению процессуальных ошибок, одна из которых – неуказание хэш-суммы цифрового файла в постановлении о назначении экспертизы и в самом экспертном заключении. Цель: проанализировать процессуальную ошибку, совершаемую следователями и экспертами при описании цифрового следа; обозначить важность указания хэш-суммы как идентифицирующей характеристики; предложить способы профилактики данной ошибки. Методы: эмпирические методы сравнения, описания, интерпретации; теоретические методы формальной и диалектической логики. Результаты: выявлена процессуальная ошибка, связанная с неграмотным описанием цифрового объекта, направляемого на экспертное исследование, а на основе анализа судебной и экспертной практики – предпосылки, ведущие к ее появлению; предложены меры по предотвращению подобных ошибок.

Ключевые слова: цифровой след, цифровой объект, цифровизация, хэш-сумма, следственная ошибка, экспертная ошибка, носитель информации, прогнозирование и профилактика ошибок

Для цитирования: Шихалиева С.З. Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме / С.З. Шихалиева. – DOI 10.33184/pravgos-2025.1.28 // Правовое государство: теория и практика. – 2025. – № 1. – С. 256–263.

Abstract. An urgent task when working with digital objects is to comply with procedural rules and regulations in appointing a forensic examination and conducting research. Failure to comply with them leads to procedural errors, one of which is the failure to specify the hash sum of a digital file in the ruling on the appointment of the expert examination and in the expert report itself. Purpose: to analyse a procedural error committed by investigators and experts when describing a digital footprint; to identify the importance of specifying the hash sum as an identifying characteristic; to suggest ways of preventing this error. Methods: empirical methods of comparison, description, interpretation; theoretical methods of formal and dialectical logic. Results: the article reveals a procedural error associated with the illiterate description of a digital object sent for expert examination, and based on the analysis of judicial and expert practice the preconditions leading to its occurrence are identified; measures to prevent such errors are proposed.

Keywords: digital footprint, digital object, digitalization, hash sum, investigative error, expert error, information carrier, forecasting and error prevention

For citation: Shikhaliyeva S.Z. The Absence of a Hash Sum as a Procedural Error Arising in a Forensic Examination When Analysing Objects in a Digital Form. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2025, no. 1, pp. 256–263. (In Russian). DOI 10.33184/pravgos-2025.1.28.

ВВЕДЕНИЕ

С появлением высокотехнологичных способов совершения «традиционных» преступлений закономерно изменились и способы отображения объектов – на смену типичным аналоговым пришли цифровые. Иначе говоря, сам процесс слеодообразования изменился вместе с переходом преступлений в цифровое пространство. Это значит, что и объекты слеодообразования предстают теперь в новом, трансформированном, цифровом виде. Новые объекты слеодообразования возникают в ответ на изменения в правовой системе, технологий, общественных запросов и криминальных тенденций. Они требуют применения современных методов и подходов для обеспечения справедливости и точности экспертного исследования.

С распространением цифровых следов и цифровых объектов как объектов судебной экспертизы неизбежно возникает ряд сложностей, связанных с их выявлением, фиксацией, исследованием, что, в свою очередь, приводит к совершению следственных и экспертных ошибок.

Р.С. Белкин экспертную ошибку определил, как «не соответствующее объективной действительности суждение эксперта или его действия, не приводящие к цели экспертного исследования, если и искаженное суждение, и неверные действия представляют собой результат добросовестного заблуждения» [1, с. 335].

Рассматривая понятие ошибки, нельзя не сказать, что их природа неоднородна, в связи с чем ошибки могут быть условно подразделены на классы. Согласно классификации, предложенной Р.С. Белкиным и Е.Р. Россинской, экспертные ошибки подразделяются на три класса:

- процессуального характера;
- гносеологические;
- деятельностные (операционные) [2, с. 172; 3].

Экспертные ошибки процессуального характера заключаются в нарушении экспертом процессуального режима и процедуры производства экспертизы. К этому классу ошибок относятся: выход эксперта за пределы своей компетенции, выражение экспертной инициативы в не предусмотренных законом формах,

обоснование выводов материалами дела, а не результатами исследования, самостоятельное собирание материалов и объектов экспертизы, несоблюдение по незнанию процессуальных требований к заключению эксперта (в том числе отсутствие в заключении необходимых по закону реквизитов) и др.

На наш взгляд, процессуальные ошибки можно подразделить на ошибки, ведущие к недействительности содержания экспертного заключения, и ошибки, ставящие под угрозу недействительность формы экспертного заключения. Например, при формулировании экспертных выводов на основе материалов дела, а не результатов проведенного исследования не будет даже экспертной ошибки, поскольку самого исследования как такового нет, соответственно, и заключение в этом случае не может быть положено в основу доказательства. Следует подчеркнуть, что процессуальные экспертные ошибки часто становятся плодом следственных и судебных ошибок, связанных с назначением судебной экспертизы и оценкой ее результатов, а значит, их целесообразно рассматривать во взаимосвязи.

ЗНАЧЕНИЕ ХЭШ-СУММЫ ЦИФРОВОГО ФАЙЛА КАК ОБЯЗАТЕЛЬНОЙ ХАРАКТЕРИСТИКИ ОБЪЕКТА СУДЕБНОЙ ЭКСПЕРТИЗЫ В ЦИФРОВОЙ ФОРМЕ

Рассмотрим ошибки, которые могут быть допущены следователем в силу такого качества цифрового следа, как легкоизменяемость. Простота внесения корректировок, умышленного изменения первоначального состояния документа, тем более при наличии современных программ и приложений, на наш взгляд, требует особого внимания и своевременной «ликвидации». Безусловно, речь идет не о том, чтобы направить все усилия на устранение возможности внесения изменений в цифровой файл в принципе. Это необходимо делать лишь в рамках представления цифрового объекта на экспертное исследование. Практически любые действия в компьютерной среде приводят к образованию цифрового следа. Аналогично этому процессу любые операции с цифровым файлом отражаются в его сводных данных – контрольной сумме, или хэш-сумме.

По данным проведенного нами анкетирования следователей по вопросу о целесообразности подсчета хэш-суммы файла при назначении судебной экспертизы и описании цифрового следа, содержащегося на носителе, около половины опрошенных в своей практике неоднократно приходилось назначать судебную экспертизу цифровых объектов. На вопрос «Считаете ли Вы необходимым предпринимать меры по защите содержания цифрового следа от изменений?» 88,9 % ответили утвердительно, 11,1 % – отрицательно. 37 % респондентов не знают, что собой представляет хэш-сумма файла, лишь 1 респондент отметил подсчет хэш-суммы как способ защиты файла от внесения изменений в качестве применяемого им инструмента. Такая статистика, на наш взгляд, негативна, при этом 77 % опрошенных считают указание хэш-суммы файла надежным способом защиты его содержания, что не может не обнадеживать. Однако только 22,2 % респондентов осуществляли подсчет хэш-суммы в своей практике.

Хэш, хэш-сумма (от англ. hash – путаница, мешанина) – последовательность символов фиксированной длины, полученная путем преобразования произвольных исходных данных (числа, текста, файла и др.) при помощи специального математического алгоритма, которая однозначно соответствует этим исходным данным, но не позволяет их восстановить¹. Согласно интернет-источникам, одним из свойств хэш-суммы является ее уникальность. Если хэшированию подвергаются разные исходные данные, пусть даже различающиеся незначительно, итоговый хэш будет разным. И наоборот: использование различных алгоритмов и программ для подсчета одних и тех же исходных данных даст один и тот же хэш. Можно сказать, что хэш-сумма представляет собой точно рассчитанный, уникальный математический образ определенного файла.

Полагаем, следует рассматривать хэш-сумму файла как значимую характеристику при работе с объектами в цифровой форме. В первую очередь стоит сразу оговориться: мы не заявляем, что контрольная хэш-сумма файла

является его идентификатором, она не указывает на оригинальность следа сама по себе. В рамках судебно-экспертного исследования хэш-сумма лишь подтверждает, что экспертом был получен именно тот файл, который ему направил правоприменитель. Таким образом, соответствие хэш-суммы файла свидетельствует о том, что в его первоначальное содержание не вносилось никаких изменений.

Со стороны следователя большая ошибка – не рассчитать хэш-сумму цифрового файла, который в дальнейшем будет направлен на исследование. В случае отсутствия базового описания файла у эксперта не будет возможности на самом деле проверить, что именно он получил в распоряжение. На целесообразность идеи применения хэш-кода обращает внимание в своих исследованиях цифровых следов И.Н. Подволоцкий, отмечая, что хэш-сумма будет подчеркивать достоверность изучаемых фактов с момента изъятия цифрового следа до направления в суд. «Постоянство суммы цифровых значений определенного электронного объекта в процессе расследования будет указывать на сохранность первоначального состояния. В процессе дальнейшей работы с представленным объектом создается его копия, которую эксперт обрабатывает в зависимости от предполагаемого методикой исследования алгоритма. Все изменения, сделанные в копии файла, эксперт фиксирует в сопроводительном протоколе к своему заключению. При соблюдении данных процедур сохраняется возможность проверки правильности действий специалиста» [4, с. 52].

Анализ зарубежной доктринальной и нормативно-правовой базы подтверждает важность подсчета хэш-суммы при работе с цифровыми файлами. Одним из значимых в зарубежной практике документов, указывающих на необходимость хэшировать цифровое доказательство, являются Федеральные правила доказывания 1975 г. Они кодифицируют доказательственное право, применяемое в федеральных судах США. Документ содержит 68 правил, интересующие нас положения находятся в разделе № 9 «Аутентификация и идентификация»: Правило 901. Установление подлинности или идентификация доказательств; Правило 902. Доказательства, подтверждающие сами себя. В частности,

¹ Энциклопедия «Касперского» [Электронный ресурс]. URL: <https://encyclopedia.kaspersky.ru/glossary/hash/?ysclid=m5crbl0mup242650144/> (дата обращения: 12.01.2025).

нас интересует Поправка № 902(14), согласно которой аутентифицировать копии данных можно с помощью процесса цифровой идентификации, обычно с использованием хэш-значений. Как и в поправке № 902(13), соблюдение данного правила возможно при участии специалиста, который бы обеспечивал грамотный процесс копирования данных².

Другой вопрос – в какой момент следователь должен посчитать хэш-сумму. В силу того, что этот показатель может измениться даже после незначительного, единичного видоизменения файла, мы полагаем, что хэш-сумму следует подсчитывать в момент обнаружения цифрового следа. Следователь может сделать это самостоятельно либо с помощью специалиста. Если не выполнить данное действие во время первого осмотра и копирования цифрового следа, в дальнейшем не будет никаких гарантий того, что подсчитанная хэш-сумма соответствует действительности. Будь то некомпетентность или умысел следователя заменить файл или случайное изменение внутренних характеристик следа при переносе на флеш-накопитель, диск или иной носитель, промедление с подсчетом хэш-суммы будет помехой для установления ее достоверности. Иначе говоря, коэффициент доверия такому показателю будет весьма низким.

Отдельное внимание стоит уделить тому, где целесообразно указывать хэш-сумму изъятых файлов. Так, контрольное значение цифрового следа предлагается указывать:

- в протоколе осмотра места происшествия, в рамках которого осуществляется непосредственное изъятие цифрового следа с последующим переносом на материальный носитель;
- в постановлении/определении о назначении судебной экспертизы.

На наш взгляд, хэш-сумму необходимо указывать в обоих случаях: первично – в протоколе осмотра места происшествия, затем это же значение указать в постановлении о назначении экспертизы, чтобы цепочка передаваемых сведений была достоверной и надежной. Отчасти допущение данной процессуальной ошибки связано с затруднения-

ми, возникающими у следователей при подсчете хэш-суммы.

МЕРЫ ПРОФИЛАКТИКИ ПО ПРЕДОТВРАЩЕНИЮ ПРОЦЕССУАЛЬНОЙ ОШИБКИ

Не секрет, что сама идея анализа изменений файла благодаря отслеживанию хэш-суммы не является новой, такие предложения были сделаны еще в начале 2000-х годов, однако, как можно заметить, они до сих пор не нашли закрепления на законодательном уровне. Из этого можно сделать вывод, что идеи без четкого алгоритма реализации на практике мало чем полезны. И хотя отчасти указание на необходимость делать запись в протоколе следственного действия о технических особенностях работы с электронным носителем информации при его изъятии содержится в ст. 164.1 УПК РФ, важность описания всех характеристик цифрового следа, включая его хэш-сумму, никак не оговаривается.

В связи с этим предлагаем рассмотреть возможность разработки правил/рекомендаций процедуры изъятия и фиксации цифровых доказательств и следов в ходе следственных действий, куда можно было бы включить следующие положения.

1. Указание на обязательность участия специалиста при осуществлении операций с цифровыми следами. Данное положение обусловлено тем, что специфика работы с цифровыми следами предполагает знание всех особенностей техники изъятия, фиксации и переноса таких объектов, поскольку даже одно неосторожное движение может привести к утрате части свойств следа либо его полному уничтожению. В подтверждение этому можно привести следующую точку зрения: «Итак, ключевым этапом в выстраивании стратегии доказывания определенных фактов на основе цифровых следов являются поиск и сохранение таких следов способами, обеспечивающими относимость, допустимость и полноту доказательств. Важно понимать, что, как и где искать. Цифровые следы порождаются самыми разными процессами. Они могут представлять собой сетевые временные файлы с расширениями html, текстовые документы в форматах txt, docx, журналы

² Federal Rules of Evidence [Электронный ресурс]. URL: <https://www.rulesofevidence.org/fre/article-ix/rule-902/> (дата обращения: 12.01.2025).

системы, почтовые архивы и т. д. Их можно умышленно или неумышленно скрыть, уничтожить, изменить, зашифровать. Для доступа к таким следам требуются не только специальные знания и навыки, но и специализированное криминалистическое оборудование и программное обеспечение. Соответственно, поиск цифровых следов необходимо проводить при содействии специалиста с профильным образованием и опытом»³.

На это также обращают внимание В.А. Попов и А.А. Рудавин, отмечая: «Специалист, входящий в состав следственно-оперативной группы, решает более узкие задачи, связанные с использованием технико-криминалистических средств. В качестве примера обратимся к такой распространенной на практике ситуации, когда изъять тот или иной носитель информации не представляется возможным ввиду объективных причин. В подобной ситуации специалисту, участвующему в следственном действии, рекомендуется подготовить соответствующий образ файловой системы. На практике также возможно клонирование (посекторное копирование) информации с ее носителя... Основное отличие будет заключаться в том, что в специализированном оборудовании предусмотрена функция аппаратной блокировки, а также автоматизирован процесс определения аутентичности имеющейся и создаваемой информации. В случае использования иных средств создания посекторной копии или образа носителя информации, специалисту необходимо обеспечить запрет записи на носитель, с которого осуществляется получение данных и возможность осуществления контроля аутентичности имеющейся и создаваемой информации. Контроль аутентичности имеющейся и создаваемой информации можно осуществлять путем расчета хэш-функций (контрольных значений). В протоколе должны быть отражены способы создания и контрольные значения» [5, с. 182].

2. Обязательное указание всех важных характеристик изъятых цифровых следов, включая его размер, разрешение, хэш-сумму.

³ Особенности криминалистической фиксации цифровых доказательств и следов [Электронный ресурс]. URL: https://zakon.ru/blog/2022/08/09/osobennosti_kriminalisticheskoy_fiksacii_cifrovyyh_dokazatelstv_i_sledov/ (дата обращения: 12.01.2025).

3. Установить точный момент для подсчета хэш-суммы. Подсчет хэш-суммы копируемого и фиксируемого цифрового следа должен осуществляться в момент его обнаружения. Желательно, чтобы обнаружение и копирование файла выполнялись одновременно в целях избегания образования временного провала между тем, когда след был обнаружен, и тем, когда он фактически был скопирован на носитель, поскольку на исследование эксперт получит именно копию файла. Таким образом, следователь совместно со специалистом обнаруживает цифровой след, который необходимо извлечь для последующего исследования, фиксирует его хэш-сумму, далее переносит копию на нужный носитель. В таком случае хэш-сумма будет оставаться одинаковой, условие достоверности будет соблюдено. Эта хэш-сумма будет указана и в постановлении о назначении судебной экспертизы.

В ходе анкетирования нами была выявлена еще одна проблема, связанная с затруднениями при осуществлении подсчета хэш-суммы: 85,2 % опрошенных отметили, что хотели бы иметь инструкцию по подсчету хэш-суммы.

Проблема незнания алгоритма подсчета хэш-суммы может быть решена следующим образом: совместно со специалистами в области компьютерно-технической экспертизы может быть разработана инструкция по подсчету хэш-суммы. На сегодняшний день существует перечень надежных и апробированных алгоритмов: SHA-1, CRC32, SHA-2 и SHA-256. Более того, в некоторые операционные системы компьютеров уже включена функция автоматического подсчета данного показателя, например, в Windows 10 с помощью встроенной утилиты certutil с параметром -hashfile.

ОТСУТСТВИЕ РАССЧИТАННОЙ ХЭШ-СУММЫ ЦИФРОВОГО СЛЕДА КАК ПРОЦЕССУАЛЬНАЯ ОШИБКА СУДЕБНОГО ЭКСПЕРТА. МЕРЫ ЕЕ ПРОФИЛАКТИКИ

В самом общем виде, экспертной ошибкой является суждение эксперта, не соответствующее объективной действительности, и/или его действия, не приводящие к цели экспертного исследования, если искаженное суждение и/или неверные действия представляют собой результат добросовестного заблужде-

ния [6, с. 157]. Со стороны судебных экспертов ошибка может заключаться в следующем:

- эксперт получил сведения о хэш-сумме, но не провел самостоятельный расчет показателя, в силу чего нельзя говорить со стопроцентной уверенностью, что эксперт исследует ровно то, что ему прислали на экспертизу;

- эксперт не получил никаких сведений о хэш-сумме цифрового следа, находящегося на носителе, однако не сделал об этом пометки в ходе своего исследования.

Для выяснения мнения лиц, назначающих судебную экспертизу, была разработана анкета. Большинство опрошенных знают, что такое хэш-сумма файла, 69 % экспертов считают ее надежным способом отслеживания изменений файла, 31 % предпочли иные способы. Подсчет хэш-суммы файла осуществляют лишь 39,6 % опрошенных, что сами эксперты объяснили, помимо прочих причин, тем, что данный показатель им попросту не с чем сравнивать, поскольку изначально правоприменителем он не предоставляется, а осуществлять подсчет просто так нет смысла. На наш взгляд, такая точка зрения является оправданной, поскольку сама хэш-сумма, посчитанная экспертом, без заданной хэш-суммы от следователя/суда и без возможности их сравнения не даст никакой полезной информации.

Безусловно, контроль за тем, чтобы обеспечить неприкосновенность цифрового следа, лежит на лице, назначающем судебную экспертизу, но не стоит забывать об обязанности эксперта перед началом исследования полностью осмотреть полученные на экспертизу объекты и полноценно их описать. Последствия таких ошибок негативны, они могут привести к решению о признании заключения эксперта недопустимым доказательством.

Обнаружение экспертных ошибок и осуществление профилактических мер – два основных направления, в рамках которых можно добиться минимизации процессуальных ошибок экспертов.

Экспертные ошибки могут быть обнаружены:

- 1) при проверке самим экспертом хода и результатов проведенного исследования на любой его стадии, а на стадии формулировки выводов – особо тщательно;

- 2) при анализе и обсуждении результатов экспертного исследования, осуществляемого комиссией экспертов при производстве комиссионной и комплексной экспертиз;

- 3) при анализе экспертом или специалистом заключений предшествующих экспертиз. В данном случае, если эксперт обнаруживает ошибку в заключении предшествующей экспертизы, он принимает все меры для недопущения подобной ошибки в своем исследовании и учитывает ее при объяснении различий между своими и предыдущими выводами;

- 4) при контроле хода и результатов экспертного исследования руководителем экспертного учреждения;

- 5) следователем, присутствующим при производстве экспертизы. Если ошибка замечена следователем, присутствующим при производстве экспертизы, то он немедленно ставит об этом в известность эксперта. Однако стоит сказать, что на практике подобные случаи практически не встречаются;

- 6) при оценке заключения эксперта следователем или судом (первой, апелляционной, кассационной, надзорной инстанций). Если ошибка не влияет на выводы эксперта, она может быть нейтрализована или устранена путем допроса эксперта или назначения дополнительной экспертизы. В противном случае может быть назначена повторная экспертиза. Такое обнаружение экспертных ошибок встречается значительно чаще;

- 7) в процессе обобщения экспертной практики, осуществляемого в практических или научных целях.

Профилактические меры по предотвращению экспертных ошибок также можно условно разделить на несколько групп.

1. Меры, принимаемые экспертными учреждениями: совершенствование методического и технологического обеспечения экспертизы, создание надежной системы контроля за результатами исследования, разработка эффективной системы подготовки экспертных кадров и контроля их квалификации. Одной из наиболее значимых мер профилактики также является внутреннее рецензирование экспертными учреждениями [7, с. 13]. Об этом пишет О.Г. Дьяконова, в частности, отмечая рецензирование как одну из функций руководителя экспертного учреждения: «Приказ МВД России от 29.06.2005 № 511

предусматривает возможность со стороны руководителя организовывать выборочное письменное рецензирование заключений экспертов. Контрольная функция руководителя охватывает как судебно-экспертную деятельность организации в целом, так и действия по контролю проведения конкретных экспертиз» [8, с. 32]. Суть внутреннего рецензирования заключается в следующем: «Судебно-экспертные организации (СЭО) проверяют качество подготовленных экспертами заключений. Такое рецензирование осуществляется в рамках системы контроля за качеством экспертиз и выражается в проверке компетентными субъектами выбранной экспертом методики, ее научной обоснованности, полноты, всесторонности и логики проведенного исследования, что можно оценить положительно» [9, с. 87].

2. Меры со стороны субъектов доказывания: тщательная оценка результатов исследования и экспертных выводов. В грамотно составленном заключении эксперта должны быть указаны все необходимые реквизиты (дата, время и место производства судебной экспертизы, основания ее производства, вопросы, объекты и т. д.); выводы эксперта должны вытекать из проведенного исследования и подтверждаться им; примененные методы и методики не должны вызывать сомнений; все объекты должны быть всесторонне исследованы, а ответы эксперта – исчерпывающими и не содержать двусмысленных трактовок и т. д. Также сюда входит понимание существенных для оценки данных аспектов методологии экспертизы, ее проблемных моментов, активное привлечение специалистов, а при необходимости – назначение повторных экспертиз.

3. Меры со стороны профессионального экспертного сообщества: создание независимых комиссий, наделенных полномочиями систематически проводить внешний аудит деятельности экспертных лабораторий с целью

проверки экспертных заключений, а также соответствия квалификации персонала установленным требованиям, которые должны быть жестко регламентированы. Но этот аспект требует дополнительного исследования.

Перечисленные меры профилактики экспертных ошибок могут применяться в рамках исследования всех видов объектов.

ЗАКЛЮЧЕНИЕ

Описанные проблемы при работе с цифровыми следами – объектами судебных экспертиз позволили спрогнозировать следственные и экспертные ошибки, которые, как показывает судебная практика, могут привести к отмене судебного решения, построенного на основании судебной экспертизы, выполненной с нарушением процессуальных норм.

Как и в любой другой сфере, предотвращение ошибок возможно только путем их тщательного разбора и поиска новых путей осуществления конкретной деятельности и устранения всех предпосылок совершения таких ошибок снова. Значимость профилактики экспертных и следственных ошибок обусловлена и тем, что на сегодняшний день заключение эксперта активно используется в качестве одного из доказательств по делу. Поэтому крайне важно сделать так, чтобы такое заключение отвечало критериям достоверности, обоснованности и объективности. Также стоит отметить комплексный характер ответственности лиц, участвующих в процессе выявления и профилактики экспертных ошибок. Как было указано ранее, в этом участвуют не только эксперт, участники процесса, в том числе следователь и суд, но и экспертное сообщество. Поэтому деятельность по профилактике субъективных и объективных экспертных ошибок должна осуществляться систематически и иметь комплексный характер.

СПИСОК ИСТОЧНИКОВ

1. Белкин Р.С. Курс криминалистики : в 3 т. Т. 2. Частные криминалистические теории / Р.С. Белкин. – Москва : Юрист, 1997. – 313 с.
2. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р.С. Белкин. – Москва : Норма (Издательская группа НОРМА – ИНФРА-М), 2001. – 240 с.

REFERENCES

1. Belkin R.S. Course of Criminalistics. Moscow, Yurist Publ., 1997. Vol. 2. 313 p.
2. Belkin R.S. Criminalistics: Problems of Today. Topical Issues of Russian Criminalistics. Moscow, Norma Publ., 2001. 240 p.
3. Galyashina E.I., Golikova V.V., Dmitriev E.N. et al.; Rossinskaya E.R. (ed.). Forensic Examination: Typical Mistakes. Moscow, Prospekt Publ., 2012. 301 p.

3. Судебная экспертиза: типичные ошибки / Е.И. Галяшина, В.В. Голикова, Е.Н. Дмитриев и др. ; под ред. Е.Р. Россинской. – Москва : Проспект, 2012. – 301 с.
4. Подволоцкий И.Н. Использование цифровых технологий в деятельности экспертов / И.Н. Подволоцкий // Вестник криминалистики. – 2023. – № 4. – С. 46-58.
5. Попов В.А. Современные особенности технико-криминалистического обеспечения практики работы с цифровыми следами преступлений / В.А. Попов, А.А. Рудавин // Техничко-криминалистическое обеспечение раскрытия и расследования преступлений : сборник статей. – Москва, 2022. – С. 181–185.
6. Белкин Р.С. Криминалистическая энциклопедия / Р.С. Белкин. – Москва : БЕК, 1997. – 342 с.
7. Дьяконова О.Г. Организация профессионального сообщества судебных экспертов на основе судебной экспертологии / О.Г. Дьяконова // Судебная экспертиза. – 2023. – № 1 (73). – С. 8–21.
8. Дьяконова О.Г. О некоторых функциях руководителя судебно-экспертной организации, связанных с назначением и проведением судебной экспертизы / О.Г. Дьяконова, Е.В. Иванова // Известия Тульского государственного университета. Экономические и юридические науки. – 2022. – Вып.2. – С. 27–36.
9. Дьяконова О.Г. Рецензия специалиста на заключение судебной экспертизы и консультация специалиста: понятие, сущность, нормативное регулирование / О.Г. Дьяконова // Журнал российского права. – 2023. – Т. 27, № 4. – С. 84–97.
4. Podvolotski I.N. The Use of Digital Technologies in the Activities of Experts. *Vestnik kriminalistiki = Bulletin of Criminalistics*, 2023, no. 4, pp. 46–58. (In Russian).
5. Popov V.A., Rudavin A.A. Modern Features of Technical and Forensic Support for the Practice of Working with Digital Traces of Crimes. *Technical and Forensic Support for Detecting and Investigating Crimes. Collection of Articles*. Moscow, 2022, pp. 181–185. (In Russian).
6. Belkin R. S. Criminalistic Encyclopedia. Moscow, BEK Publ., 1997. 342 p.
7. Dyakonova O.G. Organization of a Professional Community of Forensic Experts Based on Forensic Expertology. *Sudebnaya ekspertiza = Forensic Examination*, 2023, no. 1 (73), pp. 8–21. (In Russian).
8. Dyakonova O.G., Ivanova E.V. About Some Functions of the Head of the Forensic Science Organization Related to the Appointment and Production of Forensic Expertise. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Tula State University. Economic and Legal Sciences*, 2022, iss. 2, pp. 27–36. (In Russian).
9. Dyakonova O.G. Specialist Review of the Forensic Examination Report: Concept, Essence, Regulation. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2023, vol. 27, no. 4, pp. 84–97. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Шихалиева Сельджан Заур кызы – аспирант кафедры судебных экспертиз.

INFORMATION ABOUT THE AUTHOR

Shikhaliyeva Seldjan Zaur qizi – Postgraduate Student of the Department of Forensic Examinations.

Статья поступила в редакцию 23.12.2024; одобрена после рецензирования 29.01.2025; принята к публикации 29.01.2025.
The article was submitted 23.12.2024; approved after reviewing 29.01.2025; accepted for publication 29.01.2025.