

Наджмиддинов Мухибулло Гайратджонович

КУРСАНТ АКАДЕМИЯ МВД РЕСПУБЛИКИ УЗБЕКИСТАН

Kalit soʻzlar: raqamli ekspertiza, sud ekspertizasi, raqamli dalillar, kompyuter kriminalistikasi, elektron maʼlumotlar, axborot texnologiyalari, ekspert tadqiqoti, metodologiya, maʼlumotlar yaxlitligi, ekspert xulosasi.

Annotatsiya: Maqolada raqamli ekspertizaning nazariy asoslari, uning tushunchasi, mohiyati, maqsadi va asosiy vazifalari yoritiladi. Raqamli ekspertizaning shakllanishi va rivojlanishi, uning sud ekspertizasi hamda kompyuter kriminalistikasi tizimidagi oʻrni tahlil qilinadi. Shuningdek, raqamli dalillarning xususiyatlari, ularni aniqlash, qayd etish, saqlash va tadqiq qilishning ilmiy-uslubiy tamoyillari koʻrib chiqiladi. Raqamli maʼlumotlarning yaxlitligi va ishonchliligini taʼminlash, maxsus bilimlardan foydalanish, zamonaviy axborot texnologiyalarini qoʻllash hamda ekspert xulosalarining ilmiy asoslanganligini taʼminlash masalalariga alohida eʼtibor qaratiladi. Maqolada raqamli ekspertizaning nazariy va metodologik asoslarini takomillashtirishning dolzarb yoʻnalishlari hamda uning huquqni muhofaza qilish faoliyatidagi amaliy ahamiyati ochib beriladi.

Ключевые слова: цифровая экспертиза, судебная экспертиза, цифровые доказательства, компьютерная криминалистика, электронные данные, информационные технологии, экспертное исследование, методология, целостность данных, экспертное заключение.

Аннотация: В статье рассматриваются теоретические основы цифровой экспертизы, раскрываются её понятие, сущность, цели и основные задачи. Анализируются становление и развитие цифровой экспертизы, её место в системе судебно-экспертной деятельности и компьютерной криминалистики. Особое внимание уделяется характеристике цифровых доказательств, научно-методическим принципам их обнаружения, фиксации, сохранения и исследования. Рассматриваются вопросы обеспечения целостности и достоверности цифровых данных, применения специальных знаний и современных информационных технологий, а также научной обоснованности экспертных заключений. В статье определяются актуальные направления совершенствования теоретической и методологической базы цифровой экспертизы и раскрывается её практическое значение для правоохранительной деятельности.

Keywords: digital forensics, forensic examination, digital evidence, computer forensics, electronic data, information technologies, forensic investigation, methodology, data integrity, expert conclusion.

Annotation: The article examines the theoretical foundations of digital forensics, explaining its concept, essence, objectives, and main tasks. It analyzes the formation and development of digital forensics and its role within the systems of forensic science and computer forensics. Particular attention is paid to the characteristics of digital evidence and

the scientific and methodological principles governing its identification, documentation, preservation, and examination. The article addresses the integrity and reliability of digital data, the application of specialized knowledge and modern information technologies, and the scientific validity of expert conclusions. It also identifies current directions for improving the theoretical and methodological foundations of digital forensics and highlights its practical significance for law enforcement activities.

ВВЕДЕНИЕ

Стремительное развитие информационно-коммуникационных технологий, широкое распространение электронных устройств и цифровых платформ, а также возрастающая роль электронных данных в общественных отношениях обуславливают необходимость формирования и дальнейшего совершенствования теоретических основ цифровой экспертизы. В современных условиях цифровая информация используется практически во всех сферах деятельности человека, включая государственное управление, экономику, банковскую систему, образование, здравоохранение и межличностное общение. Одновременно с этим расширяются возможности использования цифровых технологий при подготовке, совершении и сокрытии противоправных деяний, что повышает значение специальных знаний в области исследования электронных данных. В связи с этим цифровая экспертиза становится важным инструментом установления фактических обстоятельств расследуемых событий, выявления цифровых следов и получения научно обоснованных сведений, имеющих значение для раскрытия и расследования правонарушений и преступлений. Актуальность исследования теоретических основ цифровой экспертизы обусловлена прежде всего необходимостью определения её научного содержания, понятийного аппарата, принципов, задач и методологических подходов. Несмотря на активное развитие практических методов цифрового исследования, вопросы определения места цифровой экспертизы в системе судебно-экспертной деятельности, разграничения её с компьютерной криминалистикой, установления критериев достоверности цифровых доказательств и разработки универсальных принципов экспертного познания продолжают сохранять научную значимость. Решение указанных вопросов имеет принципиальное значение для обеспечения единообразия экспертной практики, повышения качества исследований и формирования обоснованных экспертных заключений. Цифровая экспертиза представляет собой направление экспертной деятельности, связанное с применением специальных знаний и научных методов для исследования цифровых данных, электронных устройств, программных комплексов и информационных систем с целью установления обстоятельств, имеющих значение для соответствующего производства. Её теоретическая основа формируется на пересечении положений общей теории судебной экспертизы, криминалистики, информатики, информационной безопасности и процессуального права. Междисциплинарный характер данного направления обуславливает необходимость комплексного подхода к определению его содержания, поскольку исследование цифровых объектов требует не только понимания технических принципов

функционирования информационных систем, но и знания закономерностей образования цифровых следов, способов их обнаружения и фиксации, а также правовых требований к получению и использованию результатов экспертного исследования. Особенность цифровых объектов заключается в том, что содержащаяся в них информация может быть представлена в различных форматах, храниться одновременно на нескольких устройствах, передаваться по сетям связи и подвергаться автоматическому изменению в процессе функционирования программного обеспечения. Цифровые данные могут содержать сведения о действиях пользователей, времени создания и изменения файлов, взаимодействиях между устройствами, использовании программ и сетевых ресурсов. Вместе с тем наличие определённой информации на электронном носителе не всегда позволяет однозначно установить её происхождение, достоверность или связь с конкретным лицом. Поэтому теоретическое осмысление природы цифровых доказательств предполагает исследование их информационных, технических и процессуальных характеристик, а также определение условий, при которых полученные сведения могут использоваться для обоснования экспертных выводов. Важнейшее значение в системе теоретических основ цифровой экспертизы имеют принципы научной обоснованности, объективности, системности, полноты исследования и проверяемости результатов. Применение данных принципов предполагает использование методов, соответствующих характеру исследуемого объекта, документирование существенных исследовательских операций, обеспечение целостности исходной информации и разграничение установленных фактов и предположений. При этом достоверность экспертного заключения определяется не только точностью применяемых технических средств, но и корректностью постановки экспертных задач, достаточностью исходных материалов, правильностью интерпретации результатов и соблюдением установленных процессуальных требований. Следовательно, развитие цифровой экспертизы требует формирования целостной теоретической системы, объединяющей общие положения экспертного познания и специальные подходы к исследованию цифровой информации. Дополнительную актуальность рассматриваемой теме придаёт постоянное совершенствование технологий хранения и обработки данных. Распространение облачных вычислений, мобильных информационных систем, криптографических механизмов защиты, искусственного интеллекта и распределённых платформ создаёт новые объекты исследования и изменяет условия получения цифровых сведений. В подобных обстоятельствах теоретические положения цифровой экспертизы должны регулярно пересматриваться и дополняться с учётом достижений науки и практики. При этом внедрение новых технических решений должно сопровождаться оценкой их надёжности, объяснимости и соответствия требованиям научной методологии. Особого внимания требует проблема соотношения технической возможности получения цифровой информации и правомерности её использования. Даже если определённые данные могут быть извлечены с помощью специализированного программного обеспечения, их исследование должно осуществляться с соблюдением применимых правовых норм и установленных пределов экспертного задания. Это

обстоятельство подчёркивает необходимость рассмотрения цифровой экспертизы не исключительно как технической процедуры, но и как особой формы применения специальных знаний в рамках регулируемой законом деятельности. Цель исследования заключается в комплексном изучении теоретических основ цифровой экспертизы, определении её сущности, основных принципов и методологических положений, а также установлении особенностей её функционирования в современной системе судебно-экспертной деятельности. Для достижения поставленной цели предусматривается решение следующих задач: раскрыть понятие и содержание цифровой экспертизы; исследовать этапы её становления и развития; определить её место в системе судебной экспертизы и компьютерной криминалистики; охарактеризовать природу и основные свойства цифровых доказательств; проанализировать научные принципы и методологические подходы к исследованию цифровых объектов; выявить основные теоретические проблемы обеспечения целостности, достоверности и проверяемости цифровых данных; определить перспективные направления развития теоретической и методологической базы цифровой экспертизы. Объектом исследования выступают общественные отношения и закономерности экспертно-познавательной деятельности, возникающие при исследовании цифровой информации в целях установления обстоятельств, имеющих юридическое значение. Предмет исследования составляют теоретические положения, научные принципы, понятийный аппарат и методологические подходы, определяющие содержание, организацию и особенности проведения цифровых экспертиз. Методологическую основу исследования образуют общенаучные и специальные методы познания, включая анализ и синтез, системный и сравнительный подходы, формально-логический метод, классификацию и обобщение научных положений. Их использование позволяет рассмотреть цифровую экспертизу как самостоятельное и одновременно междисциплинарное направление экспертной деятельности, выявить взаимосвязь между её теоретическими положениями и практическими задачами, а также определить направления дальнейшего научного развития. Теоретическая значимость исследования заключается в систематизации представлений о сущности и принципах цифровой экспертизы, уточнении её понятийных и методологических основ и раскрытии особенностей цифровых доказательств как объектов экспертного познания. Практическая значимость состоит в возможности использования сформулированных положений при разработке экспертных методик, подготовке специалистов, совершенствовании организации экспертных исследований и повышении качества заключений. Таким образом, изучение теоретических основ цифровой экспертизы является необходимым условием дальнейшего развития данного направления, поскольку научно обоснованная теоретическая база обеспечивает системность экспертного познания, способствует совершенствованию практических методов исследования и повышает надёжность использования цифровой информации при расследовании и судебном рассмотрении дел.

ОСНОВНАЯ ЧАСТЬ

1. Понятие, сущность и место цифровой экспертизы в системе научного знания. Теоретическое осмысление цифровой экспертизы предполагает прежде всего определение её понятия, сущности, целей и места в системе судебно-экспертной деятельности. В условиях цифровой трансформации общественных отношений электронная информация становится значимым источником сведений об обстоятельствах различных событий, в том числе правонарушений и преступлений. Это обуславливает необходимость применения специальных знаний для выявления, сохранения, исследования и интерпретации цифровых данных. В научном контексте цифровую экспертизу целесообразно рассматривать как направление экспертной деятельности, основанное на применении специальных знаний в области информационных технологий, компьютерной криминалистики и смежных дисциплин для исследования цифровых объектов и установления фактов, имеющих значение для соответствующего производства. При этом конкретное содержание данного понятия зависит от национального законодательства, используемой научной терминологии и характера решаемых экспертных задач. Важно учитывать, что цифровая экспертиза не сводится исключительно к техническому извлечению информации с электронного устройства. Её содержание включает установление происхождения и характеристик цифровых данных, исследование способов их формирования и изменения, анализ взаимосвязей между отдельными информационными объектами, проверку технических гипотез и формирование выводов на основе полученных результатов. Следовательно, цифровая экспертиза представляет собой комплексную познавательную деятельность, в которой технические операции подчинены определённой исследовательской задаче и должны осуществляться в соответствии с научно обоснованными методами. Теоретическая специфика цифровой экспертизы заключается в необходимости объединения положений нескольких областей знания. Общая теория судебной экспертизы определяет закономерности экспертного познания, требования к исследованию объектов и принципы формирования заключения. Криминалистика предоставляет научные положения о механизмах образования следов, способах их обнаружения, фиксации и исследования. Информатика и компьютерные науки обеспечивают понимание принципов функционирования информационных систем, структуры цифровых данных и механизмов обработки информации. Информационная безопасность позволяет учитывать особенности шифрования, разграничения доступа, сетевого взаимодействия и защиты электронных ресурсов. Процессуальное право устанавливает требования к назначению экспертизы, предоставлению материалов, пределам компетенции эксперта и использованию результатов исследования. Взаимосвязь указанных дисциплин формирует междисциплинарную основу цифровой экспертизы и определяет необходимость комплексного подхода к её теоретическому развитию. При этом цифровую экспертизу необходимо отличать от цифровой криминалистики в широком смысле. Цифровая криминалистика охватывает методы и процедуры выявления, сохранения, анализа и представления цифровых следов, применяемые в различных профессиональных

контекстах, включая расследование инцидентов информационной безопасности. Цифровая экспертиза в процессуальном понимании предполагает исследование, осуществляемое в установленном законом порядке уполномоченным лицом, обладающим специальными знаниями, с подготовкой соответствующего экспертного заключения. Вместе с тем эти направления тесно взаимосвязаны: методы цифровой криминалистики могут составлять методическую основу экспертного исследования, тогда как требования судебно-экспертной деятельности определяют условия их применения в конкретном процессуальном контексте. Таким образом, научное определение цифровой экспертизы должно учитывать одновременно её техническое содержание, познавательную направленность и правовой характер.

2. Становление и развитие теоретических основ цифровой экспертизы. Формирование теоретических основ цифровой экспертизы связано с развитием вычислительной техники, распространением персональных компьютеров, появлением глобальных компьютерных сетей и постепенным переходом различных сфер общественной жизни к электронным формам взаимодействия. На ранних этапах развития компьютерных технологий основное внимание уделялось исследованию содержимого электронных носителей, поиску файлов и анализу программного обеспечения. По мере усложнения информационных систем возникла необходимость изучения не только самих данных, но и обстоятельств их создания, изменения, передачи и удаления. Расширение возможностей сетевых коммуникаций привело к формированию новых объектов исследования, включая журналы сетевых событий, электронную переписку, данные веб-серверов и цифровые следы, возникающие при использовании интернет-сервисов. Последующее развитие мобильных устройств, облачных платформ, распределённых систем хранения и средств криптографической защиты существенно усложнило исследовательские задачи. Если ранее цифровые сведения преимущественно извлекались с локальных носителей, то в современных условиях они могут одновременно храниться на нескольких устройствах, синхронизироваться с удалёнными серверами и зависеть от внешних программных сервисов. В результате теоретические подходы к цифровой экспертизе стали ориентироваться на комплексное изучение информационной среды, взаимосвязей между источниками данных и условий, при которых цифровая информация может считаться достоверной и пригодной для экспертного анализа. Важную роль в развитии данной области сыграло формирование профессиональных стандартов и методических рекомендаций. В частности, международный стандарт ISO/IEC 27037:2012 посвящён руководящим принципам идентификации, сбора, получения и сохранения цифровых доказательств. Его значение заключается в систематизации подходов к первоначальному обращению с цифровыми объектами и обеспечению сохранности содержащейся в них информации. Вместе с тем данный стандарт не заменяет национального процессуального законодательства и не определяет автоматически допустимость цифровых доказательств в судопроизводстве. Его положения следует рассматривать как методическую основу, применение которой должно учитывать характер объекта, условия конкретного исследования и действующие правовые нормы. Дальнейшее

развитие цифровой экспертизы связано с внедрением специализированных программных средств, автоматизацией обработки информации и расширением возможностей анализа больших массивов данных. При этом технический прогресс обуславливает необходимость постоянного пересмотра методик и критериев оценки результатов. Теоретическая база цифровой экспертизы не может оставаться неизменной, поскольку новые технологии создают ранее неизвестные типы цифровых следов и изменяют способы хранения и обработки информации. Следовательно, развитие данной области предполагает непрерывное взаимодействие научных исследований, экспертной практики и технических разработок.

3. Цифровые доказательства как центральный объект экспертного познания. Одним из фундаментальных вопросов теории цифровой экспертизы является определение природы цифровых доказательств и установление критериев их достоверности. Цифровые данные представляют собой информацию, выраженную в форме, пригодной для обработки электронными вычислительными системами. Они могут содержать текстовые документы, изображения, видеозаписи, аудиофайлы, электронные сообщения, журналы событий, базы данных, программный код и иные информационные объекты. Особенность цифровых данных заключается в том, что их содержание не всегда может быть непосредственно воспринято человеком без использования соответствующего программного обеспечения. Кроме того, один и тот же информационный объект может существовать в нескольких копиях, иметь различные представления и подвергаться автоматической обработке. В теоретическом отношении необходимо различать цифровую информацию как технический объект, цифровой след как отражение определённого процесса или действия и цифровое доказательство как сведения, полученные и используемые в установленном законом порядке. Эти понятия взаимосвязаны, но не являются тождественными. Например, обнаруженный на компьютере файл представляет собой цифровой объект, его технические характеристики и история изменений могут рассматриваться как цифровые следы, а доказательственное значение содержащихся в нём сведений определяется с учётом обстоятельств получения, проверки и оценки в соответствующем процессуальном порядке. Поэтому наличие информации на электронном носителе само по себе не означает, что она автоматически приобретает статус допустимого и достоверного доказательства. Важнейшими характеристиками цифровых данных выступают целостность, доступность для проверки, установленность происхождения и соответствие исследуемым обстоятельствам. Целостность означает отсутствие необъяснённых изменений, способных повлиять на результаты исследования. Установление происхождения предполагает выяснение источника информации и обстоятельств её получения. Проверимость предполагает возможность оценить применённые методы, исследовательские операции и основания сформулированных выводов. Соответствие обстоятельствам дела требует установления связи между исследуемыми данными и вопросами, имеющими значение для расследования или судебного разбирательства. При этом ни одна из указанных характеристик не должна оцениваться изолированно от остальных. Например,

техническая неизменность файла не гарантирует достоверности его первоначального содержания, поскольку исходная информация могла быть недостоверной ещё до момента её сохранения. Аналогичным образом наличие метаданных не обеспечивает безусловного подтверждения авторства или времени создания файла, поскольку соответствующие сведения могут изменяться программными средствами либо формироваться автоматически. Следовательно, теоретическая оценка цифровых доказательств должна основываться на комплексном исследовании их технических характеристик, происхождения, контекста формирования и взаимосвязи с другими материалами. Особое значение имеет возможность существования нескольких альтернативных объяснений обнаруженных цифровых следов. Например, наличие определённого файла на компьютере не всегда свидетельствует о том, что конкретный пользователь лично создал его или ознакомился с его содержанием. Файл мог быть автоматически загружен, скопирован другим пользователем или сохранён в рамках работы программы. Для установления обстоятельств его появления необходимо анализировать дополнительные сведения, включая журналы событий, данные учётных записей, историю работы приложений и результаты других исследований. Такой подход позволяет избежать необоснованных выводов и обеспечивает более объективную интерпретацию цифровой информации.

4. Основные принципы цифровой экспертизы. Теоретическая система цифровой экспертизы основывается на совокупности общих принципов экспертного познания и специальных требований, обусловленных особенностями электронных данных. Одним из центральных принципов является научная обоснованность. Он предполагает применение методов, основанных на проверяемых знаниях, соответствующих исследовательской задаче и позволяющих объяснить полученные результаты. Используемые программные средства должны обеспечивать надёжную обработку информации, а их ограничения должны быть известны эксперту и учитываться при формулировании выводов. Научная обоснованность исключает механическое принятие результатов автоматизированной программы без понимания того, каким способом они получены и насколько применённый алгоритм подходит для конкретного объекта. Вторым принципом выступает объективность исследования. Она требует беспристрастного анализа исходных данных, проверки различных версий и недопущения подмены установленных фактов субъективными предположениями. Эксперт должен оценивать как сведения, подтверждающие первоначальную гипотезу, так и данные, которые ей противоречат. Если результаты допускают несколько технических объяснений, соответствующая неопределённость должна быть отражена в исследовании. Объективность особенно важна при анализе цифровых следов, поскольку одни и те же технические события могут возникать в результате различных действий пользователя или автоматических процессов системы. Третьим принципом является сохранение целостности исследуемых данных. В цифровой среде даже незначительное изменение информации может повлиять на дальнейшие результаты анализа. Поэтому теоретические положения цифровой экспертизы предусматривают необходимость минимизации изменений исходного объекта, документирования операций и

использования проверяемых копий в тех случаях, когда это технически возможно. При работе с цифровыми носителями могут применяться контрольные криптографические значения, позволяющие выявлять изменения содержимого между отдельными этапами исследования. Вместе с тем обеспечение целостности предполагает не только технический контроль, но и надлежащую организацию хранения, передачи и учёта исследуемых материалов. Не менее важен принцип системности. Цифровые данные должны исследоваться не как изолированные элементы, а с учётом связей между файлами, устройствами, программными процессами, сетевыми событиями и действиями пользователей. Системный подход позволяет выявлять закономерности, которые невозможно установить при анализе отдельного объекта. Например, временные отметки в нескольких журналах событий могут совместно указывать на последовательность технических операций, тогда как отдельная запись не позволяет сделать аналогичный вывод. При этом объединение сведений из разных источников требует проверки их независимости, сопоставимости временных характеристик и условий формирования. Принцип полноты исследования предполагает изучение всех доступных данных, имеющих значение для поставленных вопросов, в пределах экспертного задания и установленных правовых ограничений. Полнота не означает неограниченного исследования всей информации, содержащейся в электронном устройстве. Она предполагает достаточность исследовательских действий для решения конкретной задачи и необходимость учитывать как подтверждающие, так и опровергающие сведения. Важным принципом является также проверяемость результатов. Она обеспечивается документированием применённых методов, описанием существенных операций, фиксацией технических параметров и ясным изложением логики выводов. Чем полнее отражены условия исследования, тем легче другим специалистам оценить правильность применённого подхода и обоснованность экспертного заключения. Наконец, цифровая экспертиза должна осуществляться с соблюдением законности и уважением прав участников соответствующих правоотношений. Доступ к электронным данным, их извлечение и анализ должны соответствовать применимым процессуальным требованиям, правилам защиты персональных данных и пределам поставленной задачи. Совокупность перечисленных принципов формирует теоретическую основу надёжного, объективного и научно обоснованного исследования цифровых объектов.

5. Методологические основы исследования цифровых объектов. Методология цифровой экспертизы представляет собой систему принципов, подходов, методов и процедур, обеспечивающих научно обоснованное изучение цифровой информации. Её формирование связано с необходимостью адаптации общих положений судебно-экспертного познания к особенностям электронных данных. Методологический подход должен учитывать не только техническую структуру объекта, но и характер поставленного вопроса, условия формирования цифрового следа, способы его сохранения и возможные ограничения интерпретации. Важную роль играет системный подход, позволяющий исследовать цифровые объекты во взаимосвязи с информационной средой, в которой они функционировали. Например, анализ отдельного документа может потребовать

изучения его метаданных, истории изменений, программного обеспечения, с помощью которого он создавался, и связанных с ним записей в системе. При исследовании сетевого инцидента необходимо сопоставлять сведения с различных компонентов инфраструктуры, включая серверы, сетевые устройства и средства мониторинга. Системный подход обеспечивает более полное понимание обстоятельств формирования цифровых следов и уменьшает риск односторонней интерпретации. Сравнительный метод используется для сопоставления цифровых объектов, копий данных, временных отметок и результатов, полученных с использованием различных инструментов. Например, сравнение контрольных хеш-значений позволяет проверить совпадение содержимого цифровых копий, а сопоставление записей разных журналов событий может способствовать реконструкции последовательности действий. Вместе с тем результаты сравнения должны интерпретироваться с учётом особенностей используемых алгоритмов, форматов данных и условий получения информации. Само по себе совпадение отдельных технических признаков не всегда доказывает общность происхождения объектов, если соответствующие признаки могут возникать независимо друг от друга. Аналитический метод предполагает разделение сложной исследовательской задачи на отдельные вопросы, каждый из которых может быть изучен с применением подходящих технических средств. Синтетический метод, напротив, направлен на объединение результатов отдельных исследований в целостную картину. Их совместное использование позволяет перейти от обнаружения отдельных цифровых артефактов к обоснованному объяснению исследуемого события. При этом необходимо различать непосредственные результаты технических операций и выводы, сформированные на основе их совокупной интерпретации. Такое разграничение повышает прозрачность исследования и позволяет определить, какие утверждения непосредственно подтверждаются цифровыми данными, а какие представляют собой обобщение нескольких фактов. Существенное значение имеет экспериментальный метод, применяемый для проверки гипотез о функционировании программного обеспечения, возникновении цифровых следов и поведении информационных систем. В контролируемой среде эксперт может воспроизвести отдельные технические условия, выполнить определённые операции и сопоставить полученные результаты с исследуемыми данными. Однако эксперимент должен проводиться с учётом ограничений, связанных с различиями в конфигурации оборудования, версиях программного обеспечения и исходных условиях. Результат воспроизведения не следует автоматически переносить на исследуемое событие без оценки сопоставимости условий. Дополняет указанные методы анализ метаданных, изучение файловых структур, исследование системных журналов, восстановление доступных удалённых данных и применение специализированных инструментов визуализации и поиска. Выбор конкретных методов зависит от характера объекта и поставленных вопросов. Методологически правильное исследование предполагает не механическое использование максимального количества инструментов, а обоснованный выбор средств, необходимых для получения надёжного ответа. Важнейшим требованием является документирование применённых методов и

возможность оценить их влияние на результаты. Если используемый инструмент имеет известные ограничения, например не поддерживает определённый формат или не позволяет извлечь данные из зашифрованной области, это должно учитываться при определении полноты исследования. Таким образом, методология цифровой экспертизы основывается на сочетании общенаучных методов познания, специальных технических процедур и принципов проверяемости, позволяющих обеспечивать достоверность и обоснованность результатов.

6. Теоретические проблемы установления достоверности и целостности цифровых данных. Одной из наиболее сложных проблем теории цифровой экспертизы является определение условий, при которых цифровые данные могут рассматриваться как надёжный источник сведений о произошедшем событии. В традиционных видах экспертизы исследование нередко направлено на материальные признаки объекта, тогда как в цифровой среде значительная часть информации существует в виде логических структур и программно интерпретируемых последовательностей данных. Это усложняет непосредственное восприятие объекта и требует использования технических средств, позволяющих преобразовать информацию в форму, пригодную для анализа. При этом результат отображения может зависеть от программного обеспечения, версии приложения, настроек системы и способов обработки данных. Следовательно, эксперт должен учитывать не только содержимое исследуемого файла, но и условия, в которых оно было получено и представлено для анализа. Целостность цифровых данных обычно оценивается посредством проверки соответствия содержимого объекта на различных этапах работы. Одним из наиболее распространённых инструментов выступают криптографические хеш-функции. При вычислении хеш-значения для определённого файла или образа носителя формируется цифровой идентификатор, позволяющий обнаруживать изменения содержимого с высокой степенью надёжности при использовании подходящего алгоритма. Совпадение значений, полученных для двух объектов, является техническим основанием считать их содержимое идентичным в пределах проверяемых данных и возможностей применённого алгоритма. Однако хеширование не устанавливает автора файла, время его первоначального создания или достоверность содержащейся информации. Оно также не подтверждает автоматически законность получения данных и правильность всех предшествующих операций. Следовательно, целостность должна рассматриваться как один из элементов общей оценки цифрового объекта, а не как универсальное подтверждение его доказательственной достоверности. Дополнительную сложность создаёт проблема установления происхождения данных. Электронный документ может быть создан одним пользователем, обработан другим лицом, автоматически синхронизирован с облачным сервисом и скопирован на несколько устройств. В результате техническая история объекта может включать множество событий, не всегда доступных для полного восстановления. Метаданные, журналы событий и сведения об учётных записях помогают установить отдельные элементы происхождения, но их доказательственное значение зависит от способа формирования, сохранности и возможности независимой проверки. Например, имя пользователя, указанное в

свойствах документа, само по себе не доказывает, что именно это лицо создало файл. Аналогичным образом наличие определённой учётной записи на устройстве не означает, что все операции выполнялись исключительно её владельцем. Для повышения достоверности выводов необходимо сопоставлять разные категории сведений и учитывать альтернативные объяснения. Особое значение имеет оценка временных характеристик. Электронные устройства могут использовать различные часовые пояса, внутренние часы, автоматическую синхронизацию и форматы хранения времени. Временная отметка может отражать создание файла, последнее изменение, копирование, загрузку или другое событие в зависимости от особенностей системы. Кроме того, некоторые временные данные могут быть изменены намеренно или случайно. Поэтому восстановление хронологии цифровых событий требует анализа источников времени, технических настроек и возможных расхождений между устройствами. Без учёта этих обстоятельств существует риск формирования неправильной последовательности событий и ошибочной интерпретации взаимосвязей между цифровыми объектами. Теоретическая проблема достоверности связана также с неполнотой данных. Некоторые сведения могут быть удалены, перезаписаны, зашифрованы или недоступны вследствие ограничений используемой технологии. Отсутствие определённого цифрового следа не всегда означает, что соответствующее действие не совершалось: след мог не формироваться, не сохраняться или быть утраченным. Аналогичным образом наличие цифрового следа не всегда подтверждает завершение действия, с которым он потенциально связан. Следовательно, экспертные выводы должны учитывать не только обнаруженные сведения, но и объективные ограничения информационной среды.

7. Роль экспертного заключения в системе цифрового экспертного познания. Завершающим результатом экспертного исследования в предусмотренных законом случаях является заключение эксперта, которое отражает ход проведённой работы, применённые методы, установленные факты и выводы по поставленным вопросам. В теоретическом отношении заключение представляет собой форму представления специальных знаний, преобразованных в обоснованные выводы на основе исследования конкретных объектов. Его качество определяется не только полнотой описания цифровых данных, но и логической связью между исходными материалами, исследовательскими операциями и итоговыми утверждениями. Экспертное заключение должно позволять понять, какие сведения были получены непосредственно, какие операции проводились для их извлечения и каким образом результаты исследования обосновывают сформулированные выводы. Особенность цифровой экспертизы состоит в том, что значительная часть исследовательских операций осуществляется с применением программных средств. Поэтому в заключении важно указывать существенные характеристики использованных инструментов, версии программного обеспечения, применённые параметры и ограничения, которые могли повлиять на результат. Если исследование проводилось на криминалистической копии, необходимо отразить сведения, позволяющие установить её связь с исходным объектом и проверить целостность данных. При использовании автоматизированного анализа следует описывать, какие

действия выполняла программа и каким образом эксперт проверял полученные результаты. Такой подход позволяет избежать ситуации, когда вывод фактически основывается на непрозрачном результате программной обработки, который невозможно оценить независимо. Существенным требованием является разграничение технических выводов и правовой оценки обстоятельств. Эксперт вправе устанавливать факты, требующие специальных знаний, например наличие определённых данных, признаки изменения файла, характеристики программного обеспечения или технические обстоятельства сетевого соединения. Однако определение виновности лица, окончательная юридическая квалификация деяния и разрешение иных вопросов, относящихся к компетенции органов расследования и суда, не должны подменяться экспертным заключением. При этом даже технические выводы должны формулироваться с учётом ограничений исследования. Если представленные материалы не позволяют однозначно установить определённое обстоятельство, эксперт должен прямо указать на недостаточность данных либо обосновать вероятностный характер вывода. Необоснованная категоричность снижает научную ценность заключения и может привести к неправильной оценке доказательственной информации. Важным критерием качества является проверяемость. Она предполагает, что описание исследования содержит достаточную информацию для оценки корректности применённых методов и логики выводов. Полная повторяемость всех операций не всегда возможна из-за технических ограничений, изменения программных платформ или недоступности исходной инфраструктуры. Тем не менее надлежащее документирование позволяет другим специалистам проверить существенные этапы анализа и определить, насколько полученные результаты соответствуют исходным данным. Следовательно, экспертное заключение следует рассматривать не просто как итоговый документ, а как логически организованное обоснование результатов исследования, качество которого непосредственно зависит от соблюдения теоретических и методологических принципов цифровой экспертизы.

8. Современные направления развития теории цифровой экспертизы. Дальнейшее развитие теоретических основ цифровой экспертизы определяется появлением новых технологий, увеличением объёма цифровой информации и усложнением способов взаимодействия между информационными системами. Одним из наиболее значимых направлений является разработка общих критериев оценки достоверности цифровых данных, позволяющих учитывать особенности их формирования, хранения, передачи и преобразования. Важной задачей остаётся совершенствование классификации цифровых объектов, поскольку традиционное разделение по типам устройств не всегда отражает особенности современной распределённой инфраструктуры. Один и тот же информационный объект может одновременно существовать в локальной памяти, резервной копии, облачном сервисе и системе синхронизации, поэтому теоретические модели должны учитывать взаимосвязи между отдельными экземплярами данных и условия их изменения. Перспективным направлением является исследование возможностей применения искусственного интеллекта и машинного обучения в экспертной деятельности. Такие технологии могут использоваться для

предварительной классификации файлов, поиска сходных объектов, обнаружения аномалий и анализа больших массивов информации. Вместе с тем автоматизированные системы способны допускать ошибки, зависеть от качества обучающих данных и формировать результаты, интерпретация которых требует специальных знаний. Поэтому теоретическое развитие цифровой экспертизы должно включать определение критериев проверки алгоритмов, оценку воспроизводимости результатов и разработку требований к документированию автоматизированных операций. Принципиально важно, чтобы использование искусственного интеллекта не приводило к замене научно обоснованного экспертного анализа непрозрачными автоматическими выводами. Отдельного внимания заслуживает развитие теории исследования облачных и распределённых данных. В таких системах информация может храниться на инфраструктуре, физически расположенной в разных государствах, а доступ к ней осуществляется через программные интерфейсы и учётные записи. Это требует разработки методологических подходов, позволяющих оценивать происхождение выгруженных данных, полноту предоставленных материалов, особенности их синхронизации и ограничения доступа к первичным источникам. Кроме того, актуальной остаётся проблема исследования зашифрованной информации, новых типов электронных носителей и цифровых объектов, создаваемых автономными устройствами. Расширение интернета вещей приводит к появлению дополнительных источников цифровых следов, включая датчики, системы управления, устройства мониторинга и автоматизированные технические комплексы. Теоретические подходы к исследованию таких объектов должны учитывать специфику их функционирования, точность временных данных, способы передачи информации и возможность автоматического формирования записей без непосредственного участия человека. Не менее важным направлением выступает унификация терминологии и совершенствование научно-методического обеспечения. Единообразное использование понятий «цифровой след», «цифровые данные», «цифровое доказательство» и «цифровая экспертиза» способствует более точному научному обмену и уменьшает риск неоднозначного толкования результатов. При этом унификация должна учитывать различия национальных правовых систем и не подменять требования конкретного законодательства универсальными техническими рекомендациями. Развитие теоретических основ цифровой экспертизы также предполагает расширение междисциплинарных исследований, объединяющих специалистов в области криминалистики, компьютерных наук, информационной безопасности и права. Такое взаимодействие позволяет формировать более полные модели цифрового экспертного познания, совершенствовать методики исследования и повышать обоснованность экспертных заключений. В конечном счёте дальнейшее развитие цифровой экспертизы должно быть направлено на создание научно обоснованной, методологически последовательной и технически адаптивной системы исследования цифровых объектов, способной отвечать требованиям современной правоприменительной практики.

ЗАКЛЮЧЕНИЕ

В результате проведённого исследования установлено, что цифровая экспертиза представляет собой важное и динамично развивающееся направление судебно-экспертной деятельности, обусловленное широким распространением информационных технологий и увеличением количества правонарушений, связанных с использованием цифровых устройств, электронных данных и информационных систем. Её теоретические основы формируются на пересечении положений общей теории судебной экспертизы, криминалистики, информатики, информационной безопасности и других научных дисциплин. Такое междисциплинарное взаимодействие определяет специфику цифровой экспертизы, содержание её методов и требования к результатам экспертного исследования. В ходе рассмотрения теоретических аспектов цифровой экспертизы выявлено, что её предметное содержание не ограничивается исследованием компьютерной техники или отдельных электронных файлов. Оно охватывает установление фактических обстоятельств, связанных с созданием, хранением, изменением, передачей и использованием цифровой информации, а также выявление закономерностей формирования и сохранения цифровых следов. При этом особое значение приобретают научно обоснованные подходы к обнаружению, фиксации, изъятию, сохранению и анализу цифровых объектов, поскольку любые нарушения установленной последовательности действий могут привести к утрате значимой информации либо поставить под сомнение достоверность полученных результатов. Установлено, что цифровые доказательства обладают рядом специфических признаков, включая нематериальную форму представления информации, зависимость от технических средств и программной среды, возможность быстрого изменения и копирования, а также необходимость применения специальных методов для их корректного исследования. В связи с этим обеспечение целостности цифровых данных, документирование каждого этапа экспертного исследования и возможность независимой проверки полученных результатов должны рассматриваться как обязательные условия качественного экспертного производства. Использование контрольных хеш-сумм, создание криминалистических копий, регистрация последовательности исследовательских действий и сохранение исходных объектов позволяют повысить надёжность результатов, однако сами по себе не заменяют комплексной оценки происхождения, контекста и достоверности цифровой информации. Важнейшим выводом исследования является положение о том, что развитие цифровой экспертизы требует не только совершенствования технических средств и программного обеспечения, но и дальнейшего формирования единой научно-методологической основы. Такая основа должна включать общие принципы экспертного познания, систематизированную классификацию цифровых объектов, научно обоснованные методики исследования, критерии оценки достоверности результатов и требования к содержанию экспертного заключения. Особое внимание необходимо уделять разграничению фактически установленных обстоятельств, результатов технического анализа и экспертных интерпретаций, что способствует объективности выводов и снижает риск ошибочного

толкования цифровых данных. Кроме того, перспективным направлением совершенствования теории цифровой экспертизы является разработка методик исследования информации, размещённой в облачных хранилищах, мобильных устройствах, распределённых информационных системах и устройствах Интернета вещей. Расширение применения технологий искусственного интеллекта и автоматизированных аналитических инструментов открывает дополнительные возможности для обработки значительных массивов цифровой информации, выявления закономерностей и обнаружения потенциально значимых следов. Вместе с тем применение таких технологий должно сопровождаться проверкой воспроизводимости результатов, оценкой возможных ошибок и обеспечением прозрачности используемых методов. Автоматизированные средства не могут полностью заменить профессиональные знания эксперта, критическую оценку исходных данных и соблюдение процессуальных требований. Практическая значимость дальнейшего развития теоретических основ цифровой экспертизы заключается в повышении эффективности расследования правонарушений, укреплении доказательственной базы и обеспечении защиты прав и законных интересов участников судопроизводства. Для достижения этих целей необходимо совершенствовать нормативное регулирование, развивать межведомственное и международное сотрудничество, обеспечивать профессиональную подготовку экспертов и регулярно обновлять методические рекомендации с учётом изменений в информационных технологиях. Не менее важным условием является согласование национальных подходов с признанными международными стандартами при обязательном соблюдении требований национального законодательства. Таким образом, теоретические основы цифровой экспертизы следует рассматривать как постоянно развивающуюся систему научных положений, принципов и методов, обеспечивающих обоснованность экспертного познания в цифровой среде. Их дальнейшее совершенствование должно быть направлено на повышение достоверности и проверяемости экспертных выводов, обеспечение сохранности цифровых доказательств и формирование единых научно-методических подходов к исследованию цифровых объектов. Последовательное решение указанных задач позволит укрепить роль цифровой экспертизы в системе судебно-экспертной деятельности и повысить её значение в обеспечении законности, правопорядка и эффективного правосудия.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРНЫЕ ИСТОЧНИКИ:

- ✧ The Rise of the Network Society
Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers.
- ✧ Security Engineering
Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Indianapolis: Wiley.

✧ Secrets

and

Lies

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.

✧ Regulating

Blockchain

Hacker, P., Lianos, I., Dimitropoulos, G., & Eich, S. (eds.). (2020). *Regulating Blockchain: Techno-Social and Legal Challenges*. Oxford: Oxford University Press.

✧ Soft

Law

and

the

Global

Financial

System

Brummer, C. (2012). *Soft Law and the Global Financial System*. Cambridge: Cambridge University Press.